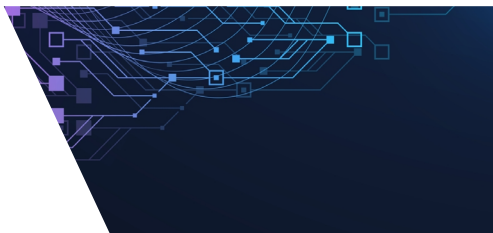
Bundesministerium
Landesverteidigung

verteidigungspolitik.at

Künstliche Intelligenz
in der Landesverteidigung



Inhalt

Die Inhalte der einzelnen Beiträge geben die persönliche Einschätzung der jeweiligen Autorinnen und Autoren wieder und entsprechen nicht notwendigerweise den Positionen des Bundesministeriums für Landesverteidigung oder den Institutionen, für die sie tätig sind.

Impressum
Republik Österreich
Bundesministerium für Landesverteidigung

Medieninhaber, Herausgeber und Hersteller:
Bundesministerium für Landesverteidigung
Roßauer Lände 1, 1090 Wien

Die Gesamtkoordination dieser Publikation erfolgte durch die Abteilung Verteidigungspolitik und Strategie.

Projektleitung und Layout:
Raphael Spötta, BA MA

Inhaltliche Koordinierung:
David Song-Pehamberger, BA MAIS

Redaktion und Lektorat:
Mag. Walter Matyas, Miriam Gruber, BA MAIS, Laura REIS, BA MSc

Fotos und Grafiken:
Heeres-Bild- und Filmstelle, Shutterstock

Druck: Heeresdruckzentrum, 1030 Wien

Erscheinungsjahr: 2025

Bitte sammeln Sie Altpapier für das Recycling.

ISBN: 978-3-902275-62-2

Shutterstock

Editorial des Generalsekretärs

Liebe Leserin, lieber Leser!

Wir befinden uns inmitten einer globalen und gesellschaftsübergreifenden digitalen Transformation, geprägt von zunehmender Vernetzung und stetig steigender Rechenleistung. Die Integration von Künstlicher Intelligenz (KI) in digitalen Prozessen aller Art führt nun dazu, dass diese Transformation zunehmend rapide und mit enormen Effizienzsprüngen voranschreitet. Hiermit sind sowohl viele Chancen, als auch bedeutende Risiken verbunden.

KI bietet besondere Chancen bei komplexen, globalen Herausforderungen, für welche bestehende Analysemodelle nicht ausreichen. Mit noch nie dagewesenen Auswertungs- und Analysemöglichkeiten großer Datenmengen durch KI-Modelle können beispielsweise neue Durchbrüche in der Medizin erreicht und die Konsequenzen des Klimawandels besser verstanden und abgefedert werden. Des Weiteren ist die zunehmende Automatisierung unzähliger Prozesse in Industrie und Verwaltung auch eine Chance, dem demografischen Wandel besser entgegenzuwirken.

Arnold H. Kammel

Dr. Arnold H. Kammel ist seit 2022 Generalsekretär im Bundesministerium für Landesverteidigung.

KI verschärft jedoch auch sicherheitspolitische Risiken in unserer Gesellschaft. Ein geopolitisches Wettrennen globaler Akteure um die Vormachtstellung in diesem und anderen Technologiebereichen hat bereits begonnen und nimmt weiter an Fahrt auf. Zunehmend komplexe und leistungsfähige KI-Modelle verschärfen somit auch die Systemkonkurrenz und gefährden den internationalen Frieden.

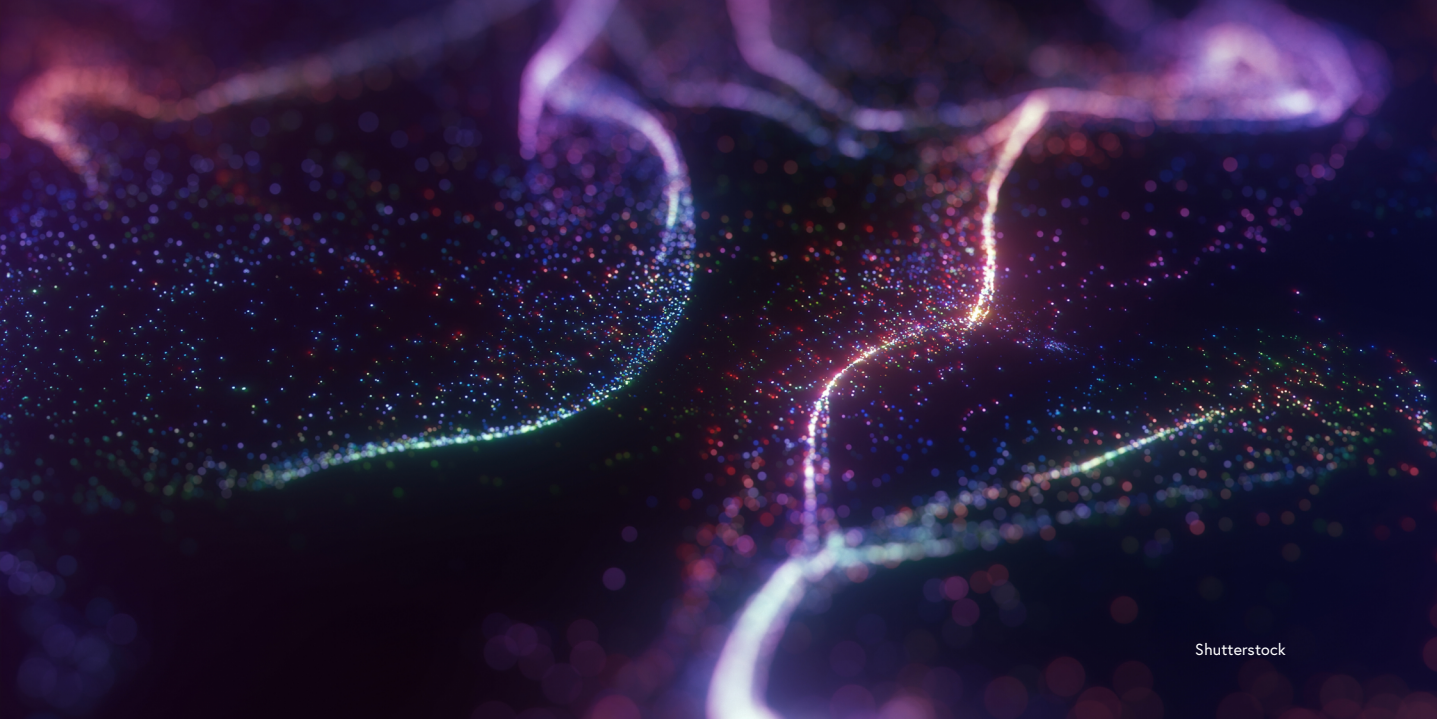
Auch unsere Landesverteidigung sieht sich mit der Tatsache dieser gesellschaftlichen Transformation und deren Herausforderungen konfrontiert. Um sich dem zu stellen, hat das Bundesministerium für Landesverteidigung (BMLV) 2024 die erste KI-Strategie des Ressorts verfügt. Diese Strategie nimmt sich der umfangreichen Thematik an und adressiert wesentliche Bestandteile der Digitalisierung, inklusive der Cyber-Verteidigung und der Datennutzung.

Da auch die beste Strategie ohne gewissenhafte Umsetzung vergeblich ist, stellt die holistische Implementierung einen besonderen Schwerpunkt der BMLV KI-Strategie dar.

Hierfür beinhaltet diese einen zehnjährigen Umsetzungshorizont, in dem KI schrittweise, nachhaltig und risikobasiert im Österreichischen Bundesheer (Fähigkeitsentwicklung) und im BMLV (Verwaltung) zum adäquaten Einsatz gebracht werden soll. KI wird hierfür nicht als Eigenzweck eingesetzt, sondern als gezielter Aspekt der digitalen Transformation der österreichischen Landesverteidigung. Auch Bedenken zur Datensicherheit und Privatsphäre sowie zunehmend ethische Fragen, die gewisse KI-Anwendungen aufwerfen, müssen sorgfältig evaluiert werden, bevor diese Anwendungen eingesetzt werden können. Darüber hinaus sind die Risikoabschätzung und strategische Vorausschau in Bezug auf KI, sowie anderen emergenten Technologien besondere Augenmerke für die kommenden Jahre, um auf die bevorstehenden technologischen Wendepunkte, samt deren Chancen und Risiken, vorbereitet zu sein.

Denn eines steht fest: Die digitale Transformation findet statt, und es liegt an uns, ob wir von ihren Chancen profitieren und den Risiken vorbereitet entgegentreten werden, oder ob wir uns von ihr überrollen lassen.

Ihr Dr. Arnold Kammel



Shutterstock

Die KI-gestützte Transformation der Streitkräfte

Rudolf Striedinger

Wir befinden uns in einer Zeit des technologischen Umbruchs. Die rasch voranschreitende Digitalisierung unserer Gesellschaft führt zur zunehmenden Vernetzung von Mensch und Maschine. Diese Vernetzung führt mithilfe immer umfangreicher werdender Sensornetzwerke zur Generierung riesiger Datenmengen. Durch die Integration von Künstlicher Intelligenz (KI) wird nun das Potenzial von großen Datenmengen und vernetzten Systeme der Informations-und-Kommunikationstechnologie (IKT) erschlossen, was zur digitalen Transformation sämtlicher Aspekte der Gesellschaft beiträgt.

Dieser Umbruch betrifft natürlich auch ganz wesentlich die militärische Landesverteidigung und somit das Österreichische Bundesheer (ÖBH), denn die Digitalisierung bietet sowohl enorme Chancen, als auch signifikante Risiken für die Streitkräfte. Aus diesem Grund befinden sich derzeit Streitkräfte weltweit in einer Phase der digitalen Transformation. Diese Transformation betrifft alle Domänen – Land, Luft, See, Weltraum, sowie den Cyber- und Informationsraum – und alle Ebenen: von der strategischen über die operative bis zur taktischen und gefechtstechnischen Ebene.

Bedeutung für das Gefechtsfeld der Zukunft

Die digitale und KI-gestützte Transformation der Streitkräfte ist eine strategische Notwendigkeit, um das moderne Gefecht zu beherrschen. Die KI-gestützte Vernetzung bietet die Möglichkeit, einst klar getrennte Domänen-Strukturen über sogenannte Multi-Domain Operations miteinander zu verbinden und somit Reaktionszeiten zu reduzieren und Effektivität enorm zu steigern, um den Anforderungen des zukünftigen Gefechtsfeldes gerecht zu werden.

Nicht nur Kommandostrukturen, sondern auch Logistik und Wartung werden zunehmend von der Sensor-Fusionierung profitieren, die somit die Effizienz der Bereitstellung erhöht und gleichzeitig die Lebensdauer von Gerätschaften und Ausrüstung verlängert. Die durch KI verbesserte Daten-Analyse ermöglicht indessen eine deutliche Effizienzsteigerung bei der Aufklärung und Lagebilderstellung sowie bei der Krisenfrüherkennung und der strategischen bis hin zur taktischen Planung.

Zunehmend ausgereifte Anwendungen der Robotik sowie autonomer Systeme bieten ebenfalls vielseitige Anwendungsmöglichkeiten, besonders in Bereichen, die für die Soldatinnen und Soldaten besondere Gefahren darstellen (z.B. Minenräumung) oder in denen die menschliche Reaktionszeit nicht ausreicht (z.B. Raketenabwehr). Im Zuge aktueller militärischer Konflikte, beispielsweise des russischen Angriffskriegs gegen die Ukraine, wird deutlich, dass Drohnen, sowohl zur Aufklärung als auch zum Kampf, bereits eine enorme Rolle auf dem Gefechtsfeld spielen und dies umso mehr in Zukunft tun werden.

Bedeutung für die Fähigkeiten des ÖBH

Abseits von der Robotik sind KI-Systeme vorwiegend Software-basierte Modelle. Dementsprechend profitiert der Bereich der Cyber-Sicherheit und Cyber-Verteidigung bereits enorm vom Einsatz von KI zum Schutz der IKT-Systeme. KI wird hier auch zunehmend zur Verteidigung gegen gegnerische KI von Bedeutung sein, da KI-Systeme bereits für automatisierte Cyber-Angriffe eingesetzt werden.

Darüber hinaus entsteht mit der Nutzung neuer, digitaler Mittel zur Ausbildung, Weiterbildung und Übung ein klarer Mehrwert für die Soldatinnen und Soldaten des ÖBH. Generative KI bietet

ebenfalls vielseitige Einsatzmöglichkeiten in diesen und anderen Bereichen, wie beispielsweise zur Übersetzung von Fremdsprachen sowie zur Analyse und Informationsgewinnung von Sprache und Text. Abschließend darf auch das Verwaltungswesen und dessen Potenzial zur Automatisierung gewisser Prozesse nicht vergessen werden. In all diesen Teilbereichen ist zu betonen, dass KI immer verantwortungsvoll eingesetzt werden und zur Unterstützung des Menschen, nicht zu dessen Ersatz, dienen muss.

Den Wegweiser für die Integration transformativer Technologien zum Aufbau und zur Ausrichtung des ÖBH für die Zukunft bietet der Aufbauplan ÖBH 2032+. Dieser bildet den militärstrategischen Rahmen, der dank der Bereitstellung notwendiger Mittel das ÖBH im kommenden Jahrzehnt zum umfassenden Schutz Österreichs befähigen wird. Trotz des Freimachens bedeutender Ressourcen für die Entwicklung des ÖBH und dessen Transformation für eine durch emergente und disruptive Technologien geprägte Zukunft stehen wir – so wie alle Streitkräfte weltweit –vor deutlichen Herausforderungen bei der Implementierung von KI.

Langfristige disruptive Entwicklungen

Derzeit schreiten die Entwicklungen auf dem Gefechtsfeld sowie der neueste Stand der Technik und Innovation so enorm voran, dass es jährlich zu bedeutenden technologischen Durchbrüchen kommt. Dieser Trend der rasanten Entwicklungszyklen nimmt weiterhin an Fahrt auf. Umfang und Ausrüstung von Streitkräften bestehen jedoch auf ausgewogener und langfristiger Planung, die auf Umsetzungshorizonten basieren, die in Dekaden gemessen werden. Um dem Trend der rapiden Entwicklung disruptiver Technologien gerecht zu werden, müssen die Zyklen von Planung und Beschaffung beschleunigt und iterativ gestaltet werden, während die bewährten Aspekte stabiler und risikobasierter militärischer Vorausschau und Planung berücksichtigt werden. Kurz gesagt: Wir müssen schneller und flexibler werden, ohne dabei die eigene Sicherheit zu riskieren.

Abgesehen von der Beschleunigung von Prozessen müssen jedoch noch andere Grundlagen beachtet werden, um die digitale Transformation effektiv und langfristig zu gestalten. Vernetzte Systeme müssen interoperabel gehalten werden, sowohl im Rahmen der eigenen Strukturen der

General Mag. Rudolf Striedinger ist seit 2022 Generalstabschef des Österreichischen Bundesheeres.

nationalen Landesverteidigung, als auch mit Partnern. Hierfür ist die internationale Zusammenarbeit ein Schlüsselelement für das ÖBH, um an Bereichen wie Standardisierung, Forschung und Entwicklung sowie gemeinsamer Beschaffung mitwirken und davon profitieren zu können. Für Österreich ist vor allem der Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) der EU hervorzuheben.

Strukturenübergreifende und ineinander verschränkte Systeme werfen jedoch auch Fragen der Vulnerabilitäten und Angreifbarkeit über den Cyber-Raum auf. Daher ist es notwendig, die digitale Transformation der Streitkräfte auf dem Prinzip von Security-by-Design umzusetzen.

Dies bedeutet, dass auf die verwendete Systemarchitektur und die Akkreditierung aller eingesetzten IKT-Systeme besonderes Augenmerk gelegt werden muss. Hier dürfen keine Abstriche gemacht werden, auch wenn dies zur Verzögerung der Einsatzfähigkeit führt.

Die Digitalisierung der Streitkräfte ist ein Prozess, der uns alle betrifft, und von dem sich niemand ausnehmen kann und darf. KI wird diesen Prozess unterstützen. Es liegt an uns, wie verantwortungsvoll wir damit in Zukunft umgehen werden, ohne Zurückhaltung, aber mit dem notwendigen Respekt vor den damit verbundenen Gefahren.


Shutterstock

Künstliche Intelligenz und hybride Bedrohungen

Die Domänen Cyber und Weltraum

Künstliche Intelligenz (KI) verfügt über das Potenzial, Konfliktlösungen zu unterstützen – in der konventionellen wie auch asymmetrischen Kriegführung, und auch in den Domänen Cyber- und Weltraum.

Josef Schröfl

KI in der Austragung hybrider Konflikte

Der Begriff hybride Bedrohungen bezieht sich auf Handlungen staatlicher oder nichtstaatlicher Akteure, die ein Ziel (z.B. Staat, Gesellschaft) durch die Kombination offener und verdeckter militärischer und nichtmilitärischer Mittel schwächen oder schädigen wollen. Hybride Konflikte, die durch eine Mischung aus konventioneller Kriegführung, irregulären und asymmetrischen Taktiken, Cyber-Operationen und Informationskrieg gekennzeichnet sind, stellen seit einigen Jahren einzigartige Herausforderungen für die Sicherheitspolitik

dar. In diesem Zusammenhang erweist sich KI als starkes Werkzeug mit dem Potenzial, die Entscheidungsfindung der Politik, Strategieentwicklung, Frühwarn- und Aufklärungssysteme sowie Vermittlungsbemühungen nach einem Konflikt zu beeinflussen.

KI wird bereits jetzt in Konflikt- bzw. Kriegssituationen eingesetzt. Beispielhaft zu nennen sind hierbei die Verwendung von sogenannten „Deepfakes" im Zuge des russischen Angriffskriegs gegen die Ukraine. Manipulierte Videos, wie etwa des ukrainischen Präsidenten, der im Rahmen einer Ansprache die europäischen Alliierten beschimpft haben soll, werden dazu verwendet, Fehlinformationen in der ukrainischen Bevölkerung zu verbreiten. So soll die Moral untergraben und das Ansehen der Regierung beschädigt werden. Weiters erfolgte wenige Stunden vor Beginn der Invasion Russlands ein Cyber-Angriff, der sich gegen das Satellitennetzwerk KA-SAT des Betreibers ViaSat richtete. Dieses Netzwerk wurde u.a. von den ukrainischen Streitkräften für ihre Command-and-Control-Systeme (C2) genutzt. Allerdings waren auch tausende zivile Kundinnen und Kunden auf dem gesamten europäischen Kontinent betroffen, einschließlich kritischer Infrastrukturen.

Einsatzmöglichkeiten bei der Konfliktlösung

KI-gesteuerte Frühwarn- und Aufklärungssysteme spielen eine entscheidende Rolle bei der Eskalationsentwicklung. Diese Systeme analysieren riesige Datenmengen, darunter Social-Media-Posts, Satellitenbilder und Kommunikationsmuster, um Anomalien beziehungsweise Muster im Zusammenhang mit potenziellen Konflikten zu erkennen. Durch rechtzeitige Warnungen unterstützt KI politische Entscheidungsträgerinnen und -träger oder bereits eingesetzte Truppen bei der Ergreifung von Präventivmaßnahmen.

Konfliktlösungen beinhalten oft komplexe Entscheidungen. KI kann Entscheidungsträgerinnen und träger unterstützen, indem historische Daten analysiert, Risiken bewertet und optimale Vorgehensweisen vorgeschlagen werden. KI-Modelle können bei Verhandlungen Strategien empfehlen, die auf historischen Fakten beruhen, aber auch kulturelle Unterschiede und die Lebensgeschichte der Beteiligten berücksichtigen.

Diplomatinnen und Diplomaten, die Frieden zwischen Konfliktparteien aushandeln, stehen oft vor der Herausforderung, einen

gemeinsamen Nenner zwischen den Konfliktparteien zu finden. KI kann Verhandlungsstrategien vorschlagen, mögliche Ergebnisse simulieren und Kompromissbereiche identifizieren. Durch die Analyse von Textdaten aus Verhandlungsprotokollen und historischen Abhandlungen kann KI Konvergenz- und Divergenzpunkte hervorheben und Verhandlungsführerinnen und -führer somit bei ihren Bemühungen unterstützen.

KI kann auch Möglichkeiten für Dialog, Versöhnung und Vertrauensbildung identifizieren. Algorithmen zur Sprachverarbeitung (NLP) analysieren Reden, Interviews und öffentliche Erklärungen, aber auch soziale Medien, um die Stimmung der Konfliktparteien (Gesellschaft, Politik, etc.) einzuschätzen, gemeinsame Werte zu identifizieren und basierend darauf vertrauensbildende Maßnahmen zu empfehlen.

KI-Modelle simulieren Konflikt- bzw. Kriegsszenarien und ermöglichen somit den politischen Entscheidungsträgerinnen und -trägern verschiedene Möglichkeiten der Konfliktentwicklung abzuwägen und deren Konsequenzen einzuschätzen. Durch die Anpassung von Variablen wie z.B. Truppenbewegungen, Wirtschaftssanktionen oder Cyber-Angriffen erhalten sie Einblicke in deren mögliche Auswirkungen. Diese Simulationen dienen der Strategieentwicklung, aber auch dem Krisenmanagement.

Um KI letztendlich vertrauensbildend einsetzen zu können, sind Transparenz und logische Erklärbarkeit entscheidend. Transparente KI-Systeme sind das Ziel von Demokratien, in Autokratien wird KI eher stillschweigend und an der Gesellschaft vorbei eingesetzt. Hier hat die Europäische Union mit der Verordnung über Künstliche Intelligenz („AI Act“) bereits ein Zeichen gesetzt.

Es ist von größter Bedeutung, sicherzustellen, dass KI-Systeme ethischen Richtlinien entsprechen. Voreingenommenheit, Diskriminierung und unbeabsichtigter Schaden müssen minimiert werden. Allerdings lernen KI-Algorithmen auch aus historischen Daten, die Verzerrungen enthalten können. Um diese zu mildern, muss KI dauerhaft trainiert und kontinuierlich überwacht werden. Effektive Konfliktlösungen erfordern ein Gleichgewicht zwischen menschlicher Expertise und KI-Fähigkeiten. Obwohl die KI riesige Datenmengen verarbeiten kann, bleiben menschliches Urteilsvermögen, Empathie und kulturelles Verständnis unersetzlich.

KI in den Domänen Cyber und Weltraum

Durch die Digitalisierung ist der Weltraum immer stärker mit dem Cyber- und Informationsraum verknüpft worden. Satelliten, Bodenstationen und Benutzerterminals sind Cyber-Bedrohungen zunehmend ausgesetzt. Das Verständnis der Verbindungen zwischen Cyber- und Weltraum ist entscheidend, um die Weltraumressourcen, auf die sich die Gesellschaft verlässt, zu schützen.

Satelliten können wie jedes digitale Objekt gehackt werden. Da sie jedoch so weit vom Alltag der meisten Menschen entfernt sind, kann ihre Bedeutung und die Abstützung der Gesellschaft auf diese kritische Weltraum-Infrastruktur leicht übersehen werden. Ein Cyber-Angriff auf einen Satelliten kann gleichzeitig die Finanzmärkte, den Straßenverkehr, Wettervorhersagen, Internetverbindungen, Stromnetze, die Flugsicherung und militärische Operationen erheblich beeinträchtigen.

Astronominnen und Astronomen haben oft mit riesigen Datenmengen von Teleskopen und Satelliten zu tun. KI hilft bei der Verarbeitung dieser Daten, bereinigt verrauschte Bilder und extrahiert nützliche Informationen. Beispielsweise wurde das Wissen über das größte schwarze Loch im Zentrum der Galaxie Messier 87 (M87) mithilfe der KI verbessert, wodurch eine klarere Ansicht seiner Struktur entstand. Zudem kann KI Missionsplanungen rationalisieren, indem beispielsweise Flugbahnen, Ressourcenzuweisung und Zeitplanung optimiert werden. Sie verbessert weiters auch die Satelliteneffizienz durch Automatisierung von Aufgaben, beispielsweise durch optimale Satellitenpositionierung.

Zusammenfassend lässt sich sagen, dass KI die Weltraumforschung revolutioniert, sie schneller und effizienter macht und Entdeckungen ermöglicht, die über das hinausgehen, was der Mensch allein hätte erkennen können. Mit der Entwicklung der Bedrohungslandschaft im Weltraum sollte sich auch das Verständnis der Cyber-Risiken und ihrer Minderungsmaßnahmen zum Schutz der Weltraumressourcen und der breiten Palette von Diensten, die sie der Gesellschaft bieten, weiterentwickeln. Zukünftige Herausforderungen in der Cyber-Sicherheit im Weltraum werden darin bestehen, die Qualifikations- und Informationslücke zu schließen und herauszufinden, wie Cyber-Operationen im Weltraum am effektivsten durchgeführt werden können und

wie darauf reagiert werden kann. Ebenso ist festzuhalten, dass KI bei der Lösung hybrider Konflikte eine wichtige Rolle spielen kann.

Trotz aller Hindernisse kann der verantwortungsvolle Einsatz von KI zu einer Verbesserung bei der Konfliktprävention, Entscheidungsfindung und Friedenskonsolidierung beitragen.

Oberst Josef Schröfl ist stv. Direktor am Hybrid Centre of Excellence in Helsinki, Finnland.

Shutterstock

Künstliche Intelligenz im Militär und am Gefechtsfeld

Ausblick und Zukunftstrends

Der Einsatz von Künstlicher Intelligenz (KI) in Streitkräften und auf dem Gefechtsfeld wird in den nächsten 10 Jahren nicht nur linear, sondern exponentiell wachsen. Dies wird aktuell noch systematisch unterschätzt. Der Schritt von einem „Kampf der verbundenen Waffen" zu einem „All Domain Mosaic warfare" ist ein großer, der auf allen Ebenen von KI dominiert werden wird.

Joachim Klerx

KI steigert nicht nur die Effizienz und die Geschwindigkeit des Kampfes, sondern auch die Geschwindigkeit und Effizienz der Erforschung neuer Methoden zum Kampf. Zivile KI-Systeme werden vielfach als wichtigste Zukunftstechnologie, aber auch immer wieder als größte Bedrohung der Zukunft betrachtet. Sogar führende Persönlichkeiten der KI-Entwicklung wie Sam Altman (OpenAI) und Elon Musk (xAI, Tesla) warnen vor den Risiken von

KI und gefährlichen Innovationen. Dasselbe gilt für militärische KI-Systeme, vor allem wenn es um die Frage geht, wie sich das Gefechtsfeld durch solche Entwicklungen verändern wird.

In naher Zukunft

Die Steigerung der Effizienz, Leistungsfähigkeit und der „Intelligenz" von KI-Systemen ist ein zentraler Trend. Aktuelle Systeme mit sogenannter „schwacher KI" (Narrow AI) sind auf spezifische Aufgaben optimiert. Die Hauptcharakteristik von schwacher KI ist ihre Spezialisierung. Diese Systeme können nur jene Aufgaben erfüllen, für die sie programmiert wurden, und sind nicht dazu in der Lage, darüber hinaus zu lernen oder zu handeln. Ihr Vorteil ist, dass sie Echtzeit-Informationen von verschiedenen Sensoren und Quellen verarbeiten und in ihrem Bereich sehr schnell Entscheidungen auf einer komplexen Datengrundlage treffen können.

In der militärischen Nutzung wird schwache KI für Anwendungen wie Aufklärung, automatisierte Überwachung, Zielerkennung und im Cyber-Bereich eingesetzt. Weitere Beispiele sind zunehmend auch mit KI ausgestattete Roboter, die den Menschen unterstützen oder in gefährlicher Umgebung ersetzen. Auch die Optimierung von Nachschubrouten und Lagerbeständen zählt – neben vielen weiteren Anwendungen – zu den zentralen Einsatzbereichen.

Neuere, allgemeine Systeme sind zu adaptivem Lernen mit umfangreichem Kontextwissen und statistischen Methoden fähig. Durch Datenanalysen können sie Prognosen über gegnerische Bewegungen erstellen und daraus sowohl taktische als auch strategische Entscheidungen für den Einsatz ableiten. In naher Zukunft werden sich KI-Systeme zunehmend von der Unterstützung hin zur Übernahme menschlicher Aufgaben entwickeln, da sie mit besserer Effizienz unter optimalem Einsatz von Ressourcen analysieren, vorhersagen, planen und umsetzen können. Auf dem Gefechtsfeld werden zunehmend-autonome Waffensysteme auftauchen, die Soldatinnen und Soldaten mit ihren korrespondierenden Waffensystemen überlegen sind.

Mittelfristig

Der Übergang von schwacher KI hin zu allgemeiner Künstlicher Intelligenz (AKI) stellt einen gewaltigen Entwicklungssprung dar, dessen genauer Pfad bislang noch nicht vollständig erforscht

ist. AGI bezeichnet eine Form von KI, die in der Lage ist, menschenähnliche kognitive Fähigkeiten zu zeigen, also: Probleme flexibel zu lösen, zu lernen, zu verstehen, zu planen und sich an neue Situationen anzupassen – unabhängig vom Anwendungsbereich. Zurzeit existiert AGI noch nicht.

Es ist noch offen, ob AGI-Systeme aus neuartigen, dem Menschen nachempfundenen neuronalen Netzen bestehen, oder ob diese aus einer neuartigen Kombination von beschränkten KI-Systemen modular aufgebaut werden können. Soweit bisher bekannt, bedeutet dies für militärische AGI-Systeme vor allem, dass sie ein auf ihren Verantwortungsbereich abgestimmtes Situationsbewusstsein entwickeln, das in Bezug auf die jeweiligen Fähigkeiten zur Prognose und zur Entscheidungsunterstützung dient. Diese Fähigkeiten werden dazu beitragen, unterschiedliche Führungsebenen in der Planung zu unterstützen oder zu ersetzen.

Unabhängig von der konkreten technologischen Lösung wird eine allgemeine KI früher oder später militärisches Führungspersonal dabei unterstützen, die taktische und strategische Planung zu optimieren. Dies funktioniert mit Hilfe der Sensordaten von sogenannten „smart devices“,also elektronischen Geräten, die mit Sensoren, Prozessoren und häufig auch Internetverbindung ausgestattet sind. Diesen ist es möglich, eigenständig Daten zu erfassen, zu verarbeiten und mit anderen Geräten oder Nutzerinnen und Nutzern zu kommunizieren.

Schon jetzt werden Teile der Einsatzplanung der USA mit KI simuliert und optimiert. Eine militärische AGI würde dies in Echtzeit bewältigen. Damit steigt allerdings auch das Risiko für einen „Flash War“, einer speziellen Form sich gegenseitig eskalierender KI-Systeme, die auf die Trigger-Werte der jeweils anderen Systeme fatal reagieren. Dieses Phänomen hat sich zuerst beim Hochfrequenzhandel an den Aktienmärkten gezeigt und sollte bei Entwicklung und Einsatz militärischer AGI als Risiko berücksichtigt werden. AGI-Systeme werden wohl als „Digital Twins“ bzw. „Digital Companion“ auf dem Gefechtsfeld auftauchen und in Führungsunterstützungssystemen die Planung übernehmen.

Langfristig: superintelligente militärische KI-Systeme

Der Schritt zu einer militärischen AGI erscheint mühsam, hat aber

absehbare Folgen. Der Schritt von AGI zu ASI (Artificial Super Intelligence; eine Art von künstlicher Intelligenz, die dem Menschen in allen kognitiven Fähigkeiten weit überlegen ist.) hingegen wird vermutlich klein und unbedeutend erscheinen, jedoch weitgehend unabsehbare Folgen mit sich bringen. Die Grundlage könnte z.B. eine militärische Plattform sein, die „Smart Devices" auf dem Gefechtsfeld in ein Joint All-Domain Command and Control (JADC2; Vernetzung und integrierte Führung über alle Einsatzdomänen hinweg) integriert, wie z.B. LatticeOS (Anduril). Da bisher noch keine KI mit ASI-Fähigkeiten existiert, ist die militärische Wirkung schwer abzuschätzen.

Letale autonome Waffensysteme könnten durch die Kombination von „Smart Devices", Internet of Battelfield Things (IoBT) und ASI effektiver werden. Die ASI würde die Führung übernehmen und unbemannte Drohnen und „Smart Devices" in Echtzeit steuern, ihnen ermöglichen, sich an verändernde Bedingungen anzupassen, und ihre Missionen effizient und präzise durchzuführen. Neuromorphe Computer und Quantencomputer könnten die Reaktionszeiten dieser Systeme weiter verkürzen und ihre Entscheidungsfähigkeit verbessern.

In der Cyber-Kriegführung könnte eine ASI sowohl defensive als auch offensive Operationen auf ein neues Intensitätsniveau heben. Sie könnte Cyber-Angriffe in Echtzeit erkennen und abwehren, Schwachstellen in gegnerischen Systemen finden und ausnutzen sowie neuartige hochentwickelte Cyberwaffen entwickeln und einsetzen. Die KI-Systeme des Gegners wären ein bevorzugtes Ziel.

Ein Staat, der sich nicht am Wettbewerb um die beste militärische KI beteiligt, könnte militärisch und strategisch erheblich ins Hintertreffen geraten. Technologisch fortschrittliche Staaten werden durch den Einsatz von KI in der Lage sein, Informationen schneller und präziser zu verarbeiten, was zu besseren strategischen Entscheidungen und einer schnelleren Reaktionszeit führt. Ohne diese Technologien könnte ein Staat seine Verteidigungsfähigkeit verlieren, was ihn für moderne Bedrohungen wie Cyber-Angriffe und hybride Kriegführung anfälliger macht. Insgesamt könnte ein Staat, der bei der KI-Entwicklung zurückbleibt, sowohl strategisch, wirtschaftlich als auch außenpolitisch an Bedeutung verlieren.

Dr. Joachim Klerx ist am Austrian Institute of Technology im Bereich der Entwicklung und Erforschung von KI zur Unterstützung von Strategic Foresight tätig.

Shutterstock

Anwendungsgebiete von KI im Militär

Der Einsatz von Künstlicher Intelligenz (KI) in den Streitkräften hat das Potenzial, Effizienz und Effektivität in allen Teilbereichen zu stärken. Von der strategischen und operativen Planung bis hin zum taktischen Umfeld sowie weit über den Einsatz hinaus werden KI-Anwendungen schrittweise zur digitalen Transformation der Landesverteidigung beitragen. Diese Transformation ist bereits im Gange und wird in ihrem Gesamtumfang mehrere Jahrzehnte in Anspruch nehmen. Es gilt hierbei zwischen Automatisierung und Autonomisierung zu unterscheiden, wobei der Großteil der kurz- bis mittelfristigen Vorteile der Implementierung von KI-Modellen aus der Automatisierung bestehender Prozesse resultieren wird.

David Song-Pehamberger

Führungs- und Informationssysteme

Militärische Führungs- und Informationssysteme (Command and Control, C2) waren immer schon auf zeitgerechte und qualitativ hochwertige Daten zur Entscheidungsfindung sowie effektive Kommunikationskanäle zur Weitergabe von Befehlen angewiesen. KI-gestützte Systeme und Sen-

sor-Netzwerke ermöglichen nun die effektive und domänenübergreifende Vernetzung von einst getrennten C2-Systemen. Von der taktischen Ebene können Daten in Echtzeit an die operativen und strategischen Ebenen übermittelt, mittels KI-Modellen analysiert und zur Führungsunterstützung bereitgestellt werden. Die mögliche Geschwindigkeit dieser Prozesse übertrifft menschenmögliche Prozesse bei weitem und ermöglicht somit Entscheidungsträgerinnen und -trägern sowie Analystinnen und Analysten einen besseren Überblick und die Möglichkeit, sich auf die wichtigen Entscheidungen zu konzentrieren. Die Entscheidungen der Führungsebene können auch direkt in die Zielfindung und -bekämpfung (Targeting Cycle) einfließen. Hiermit werden Multi-Domänen-Operationen (MDO) ermöglicht, die weit über traditionelle Entscheidungs- und Kommunikationsketten hinausgehen. Dazu muss jedoch auch der Zugang zu großen und qualitativen Datenmengen mittels Sensor-Netzwerken und Aufklärung gewährleistet sein.

Nachrichtendienste und Aufklärung

KI-Systeme üben bereits einen großen Einfluss auf den Umfang und die Qualität von Information aus, die durch Nachrichtendienste und militärische Aufklärung, insbesondere im Teilbereich der Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) bereitgestellt werden. Dies stellt auch eine Grundvoraussetzung für MDO-Systeme dar. Aufgrund stetig wachsender Sensor-Netzwerke und Datenströme stehen Nachrichtendienste vor der Herausforderung, große Informationsmengen durchsuchen zu müssen. KI-Systeme können die automatisierte Mustererkennung unterstützen, um sowohl Effektivität als auch Effizienz von ISTAR drastisch zu steigern. Ein Beispiel ist die Nutzung von satellitengestützten Sensoren zur automatisierten Erkennung militärisch relevanter Truppenkonzentrationen oder -bewegungen.

Unabhängig von militärischen Sensoren unterstützen KI-Modelle außerdem den Bereich der Open-Source Intelligence (OSINT). Hiermit ist die nachrichtendienstliche Auswertung großer, öffentlich zugänglicher Daten gemeint. OSINT-Aufklärung bedient sich Daten sozialer Medien, traditioneller Mediennetzwerke, diverser Webseiten und anderer Datenströme, um nachrichtendienstlich relevante Muster zu erkennen und diese zur Einschätzung der Gefahrenlage, zur vorausschauenden

Planung oder zur direkten Führungsunterstützung einzusetzen. Die Ukraine hat OSINT bereits auf dem Gefechtsfeld eingesetzt, unter anderem zur Standortbestimmung russischer Truppen oder zur Identifizierung gefallener Soldatinnen und Soldaten.

Strategische Planung und Frühwarnung

Von besonderer Bedeutung sind KI-gestützte Krisen- und Frühwarnsysteme, die dazu in der Lage sind, Muster frühzeitig zu erkennen und die Führungsebene über potenzielle Bedrohungen zu informieren. Die strategische Planung kann vom Potenzial der KI-gestützten Analyse profitieren. Dies betrifft auch die Einsatzplanung sowie die Vernetzung mit anderen Teilbereichen wie der Logistik, Beschaffung und C2-Systemen. Wichtig ist hierbei, dass komplexe KI-Systeme nachvollziehbar und auf Basis qualitativer und relevanter Daten zu ihren Schlussfolgerungen kommen. Die letztendliche Analyse und Einschätzung muss jedoch immer von erfahrenen Expertinnen und Experten getätigt werden.

Cyber-Verteidigung

Die Cyber-Verteidigung ist ein Bereich, in dem KI-Systeme bereits eine bedeutende Rolle spielen. Mittels Deep-Learning-Modellen können beispielsweise IT-Systeme und Netzwerke dauerhaft und automatisiert überwacht und Anomalien, die auf Malware und Cyber-Angriffe schließen lassen, festgestellt werden. Außerdem können große Datenmengen und Software-Code analysiert werden, was der Bedrohungserkennung dient. Des Weiteren können KI-Systeme zum Aufdecken von Schwachstellen in den eigenen Systemen sowie zur Simulation von Cyber-Angriffen verwendet werden, um die Cyber-Resilienz zu stärken. Somit kann KI einen wichtigen Beitrag zur Cyber-Verteidigung leisten. Jedoch wird KI auch zunehmend offensiv eingesetzt, indem sie zur Generierung von Malware oder für automatisierte Cyber-Angriffen verwendet wird. Um derartige KI-gestützte Cyber-Bedrohungen aufzuspüren und abzuwehren, bedarf es ebenfalls der effektiven Nutzung von KI.

Robotik und Autonomie

Der Bereich der Robotik beruht zwar nicht unbedingt auf KI, der Einsatz komplexer KI-Systeme

ermöglicht jedoch ein zunehmend selbstständiges Agieren von Fahrzeugen (z.B. Drohnen). Ob Land-, See- oder Luftraum, um ein Fahrzeug über unwegiges Gelände zu einem gewählten Ziel zu befördern, bedarf es eines gewissen Grades an Autonomie. Die genauen Autonomiegrade sind hierfür noch nicht festgelegt, und man spricht meist von Human-in-the-Loop, Human-on-the-Loop oder Human-in-Command, je nachdem, ob das Fahrzeug einen Menschen dauerhaft, nur bei gewissen Schritten, oder nach Befehlsvergabe gar nicht mehr einbinden muss. Beim letztgenannten Autonomiegrad könnte man von vollautonomen Systemen sprechen, dennoch herrscht hierüber nach wie vor kein Konsens, da der Autonomiebegriff, insbesondere in Waffensystemen, äußerst umstritten ist. Robotik wird derzeit vor allem ferngesteuert oder teilautonom sowie in nichtletalen Bereichen wie Logistik, Minenräumung oder Aufklärung eingesetzt.

Ferngesteuerte oder teilautonome Drohnen sind bereits ein fester Bestandteil von Streitkräften. Diese haben jedoch den deutlichen Nachteil, dass sie nur in Gebieten mit aktiver Kommunikation funktionieren. Sobald die Kommunikation gestört wird (z.B. durch Jamming oder Spoofing), werden solche Fahrzeuge unbrauchbar. Deshalb werden zunehmend auch Fahrzeuge entwickelt, die nach Kommunikationsunterbrechung gewisse Funktionen (z.B. Aufklärung) bis zur Wiederaufnahme der Kommunikation selbstständig, also autonom, aufrechterhalten können. Autonom agierende Drohnen können entweder eigenständig, im Schwarm oder zur Unterstützung von bemannten Fahrzeugen (Human-Machine-Teaming) eingesetzt werden.

Wartung und Logistik

KI-Systeme können die militärische Wartung und Logistik unterstützen sowie bei der Planung und Durchführung von Bevorratung helfen. Im Bereich der Wartung kann durch die Integration von Sensoren und die Vernetzung von Systemen die Wartungsnotwendigkeit besser vorhergesagt und somit der Wartungszeitraum verkürzt als auch die Lebensdauer von Geräten verlängert werden (Predictive Maintenance). Dies kann wiederum in intelligente Lagerlösungen (Smart Warehouse) einfließen, wodurch der Bestand von Zubehör und Ersatzteilen gesichert und gleichzeitig minimiert werden kann. Auch Kasernen und militärische Liegenschaften im In- und Ausland können durch intelligente Lösungsansätze zunehmend

David Song-Pehamberger, BA MAIS, ist in der Abteilung Verteidigungspolitik und Strategie des BMLV mit Arbeitsschwerpunkt Cyber-Verteidigung, KI und emergente und disruptive Technologien tätig.

effizient, nachhaltig und autark gestaltet werden (Smart Camps).

Verbesserte Wartung und Bereitstellung fließt in die komplexe Planung der Logistik ein, die ebenfalls von der Vernetzung von Systemen und Integration von KI-gestützten Systemen in die Planung profitiert. Hierfür können Versorgungsketten optimiert und gleichzeitig resilient gestaltet werden. Dies ist aufgrund der sich oftmals rasch ändernden Umfeldbedingungen in militärischen Missionen bzw. Operationen erforderlich, da dies eine Umplanung der Versorgungsketten notwendig macht. Diese Umplanung kann durch die Integration von KI stark beschleunigt werden.

Ausbildung und Übung

Weitere Teilbereiche, in denen KI einen großen Effizienzgewinn verspricht, sind Ausbildung und Übung. Durch KI-gestützte Simulationen werden realistischere und flexiblere Ausbildungsszenarien ermöglicht, und es ist möglich, weite Bereiche des Ausbildungswesens zu digitalisieren. Übungen stellen eine relevante Grundlage für Streitkräfte zur Vorbereitung auf den Ernstfall dar. Mit KI kann die Führungsebene die Effektivität von Planspielen verbessern.

Soldatinnen und Soldaten können sich, beispielsweise durch die Einbindung von augmentierter und virtueller Realität, noch besser auf den Einsatz vorbereiten. Des Weiteren kann Fachpersonal adaptive und personalisierte Trainings durchführen, um auf dem neuesten Stand des jeweiligen Spezialgebiets zu bleiben.

Fazit: KI in allen Teilbereichen der Landesverteidigung

Die Anwendungsmöglichkeiten von KI-gestützten Systemen gehen noch weiter über die hier genannten Bereiche hinaus. Personalverwaltung, Sanitätswesen, Abrüstung und viele andere Teilbereiche und Einzelanwendungen werden ebenfalls von der Integration von KI-gestützten Systemen profitieren. Darüber hinaus ermöglicht KI die zunehmende Vernetzung der unterschiedlichen Domänen und Ebenen. Die Ergebnisse dieser KI-gestützten Transformation und Vernetzung werden rasant voranschreiten.

Shutterstock

Der rechtliche Rahmen für den Einsatz von KI im militärischen Bereich

Das bestehende Recht, einschließlich des Humanitären Völkerrechts (HuVR) im Falle eines bewaffneten Konflikts, ist auf den Einsatz von Künstlicher Intelligenz (KI) im Militär voll anwendbar und kann einen verantwortungsvollen Einsatz derartiger Systeme gewährleisten. Dabei ist zu unterscheiden, ob ein KI-Einsatz in Friedenszeiten oder in Zeiten eines bewaffneten Konflikts erfolgt, da je nach Situation unterschiedliche Bestimmungen zur Anwendung kommen.

Alexandra Duca

Rechtliche Vorgaben in Friedenszeiten

In Friedenszeiten richtet sich die Rechtslage über den Einsatz von KI nach dem nationalen Recht eines Staats. Davon umfasst sind insbesondere auch die im betroffenen Staat jeweils geltenden Grundrechte. Österreich hat alle von den Vereinten Nationen (VN) bisher entwickelten völkerrechtlichen Menschenrechtsübereinkommen ratifiziert und schützt Menschenrechte in der Verfassung und in zahlreichen einfachen Geset-

zen. Die Europäische Menschenrechtskonvention (EMRK) hat in Österreich Verfassungsrang. Die Grundrechte müssen auch beim Einsatz von KI respektiert und geschützt werden, sofern gesetzlich kein Eingriff erlaubt ist. Im militärischen Bereich ist dabei insbesondere das Militärbefugnisgesetz (MBG) zu berücksichtigen.

Das MBG bezieht sich ausschließlich auf ein Tätigwerden militärischer Organe im Bereich der militärischen Landesverteidigung (Art. 79 Abs. 1 B-VG). Es ist denkbar, dass KI im Rahmen der allgemeinen Einsatzvorbereitung, der unmittelbaren Vorbereitung eines Einsatzes sowie eines Einsatzes selbst samt Abschlussmaßnahmen eingesetzt wird. Im Wachdienst könnte KI sowohl bei der Befugnisausübung – z.B. Überwachung, (Identitäts-)Kontrolle von Personen, Betreten von Grundstücken – als auch bei der Durchsetzung der Wachbefugnisse als Mittel zur Ausübung von Zwangsgewalt zur Anwendung kommen. Im MBG sind zu diesem Zweck ausdrücklich auch Hilfsmittel der körperlichen Gewalt (u.a. Computersysteme) vorgesehen. Darüber hinaus könnte KI auch für die Aufgaben der militärischen Nachrichtendienste im Bereich der Informationsbeschaffung und -bearbeitung eine Rolle spielen. Dabei ist jedenfalls der gesetzlich normierte Rahmen zu beachten.

Rechtliche Vorgaben in Zeiten eines bewaffneten Konflikts

Im Falle eines bewaffneten Konflikts kommt das HuVR als lex specialis zur Anwendung. Dieses Rechtsgebiet ist sodann jedenfalls auch auf den Einsatz von KI-Systemen anwendbar, da das HuVR nicht auf die eingesetzten Mittel und Methoden, sondern rein auf das faktische Vorliegen eines bewaffneten Konflikts abstellt. Wesentliche Bestimmungen des HuVR finden sich in den vier Genfer Konventionen aus 1949 (GK) sowie in den beiden Zusatzprotokollen zu den Genfer Konventionen aus 1977 (ZP).

Das HuVR hat zum Ziel, Personen, die nicht oder nicht mehr an Feindseligkeiten teilnehmen, zu schützen und die Auswirkungen und Folgen eines Konflikts generell einzuschränken. Dazu existieren vier wesentliche Prinzipien: die Unterscheidung, die Notwendigkeit, die Proportionalität und die Menschlichkeit. Jeder Angriff, der im Rahmen eines bewaffneten Konflikts stattfindet, muss daher an diesen Maßstäben gemessen werden. Das gilt naturgemäß

auch dann, wenn KI-Anwendungen eingesetzt werden.

Das bedeutet, dass stets zwischen zivilem und militärischem Bereich unterschieden werden muss, Zivilistinnen und Zivilisten sowie zivile Objekte nicht angegriffen werden dürfen und zu schützen sind.

Darüber hinaus gibt es auch im Krieg kein unbeschränktes Schädigungsrecht, jede militärische Maßnahme muss geboten sein. Ähnlich ist auch das Verursachen unnötigen Leids verboten, ebenso der Einsatz von Waffen, Geschossen und Material sowie Methoden der Kriegführung, die geeignet sind, überflüssige Verletzungen oder unnötige Leiden zu verursachen. Schließlich darf auch der vorhersehbare zivile Kollateralschaden nicht außer Verhältnis zum erwarteten konkreten und unmittelbaren militärischen Vorteil stehen.

All diese Beurteilungen müssen im Einzelfall von einem Menschen durchgeführt werden, denn die Situation eines bewaffneten Konflikts ist eine höchst dynamische, die jedenfalls sehr komplexe Formen menschlichen Urteils erfordert. Dies wird auch durch den Umstand bestätigt, dass sich das HuVR ausschließlich an Menschen richtet (z.B. Art. 57 Abs. 2 lit. a ZPI: „Wer einen Angriff plant oder beschließt […]“). Dies schließt grundsätzlich nicht aus, dass KI als Hilfsmittel für einzelne Beurteilungen eingesetzt wird, wie z.B. zur Gesichtserkennung oder zur Abschätzung des erwarteten Kollateralschadens. Jedoch bleibt der Mensch stets Entscheidungsträger und nicht die KI-Anwendung. Dies ist auch ein wesentlicher Punkt für die Verantwortungszurechnung.

Die Frage der Verantwortlichkeit

Im HuVR spielt insbesondere die Kommandantenverantwortlichkeit nach Art. 87 ZPI eine große Rolle. Demnach sind militärische Kommandantinnen bzw. Kommandanten verpflichtet, in Hinblick auf die ihrem Befehl unterstellten Angehörigen der Streitkräfte und der übrigen Personen in ihrem Befehlsbereich, Verletzungen des HuVR zu verhindern, sie erforderlichenfalls zu unterbinden und den zuständigen Behörden anzuzeigen. Kommandantinnen und Kommandanten sind auch verantwortlich zu machen, wenn diese – etwa auf Basis der von einem KI-System zur Verfügung gestellten Daten, z.B. mittels KI vorgenommene Einteilung in Zivilistinnen und Zivilisten bzw. Kombattantinnen und Kombattanten – einen Angriff autorisieren, ohne diese

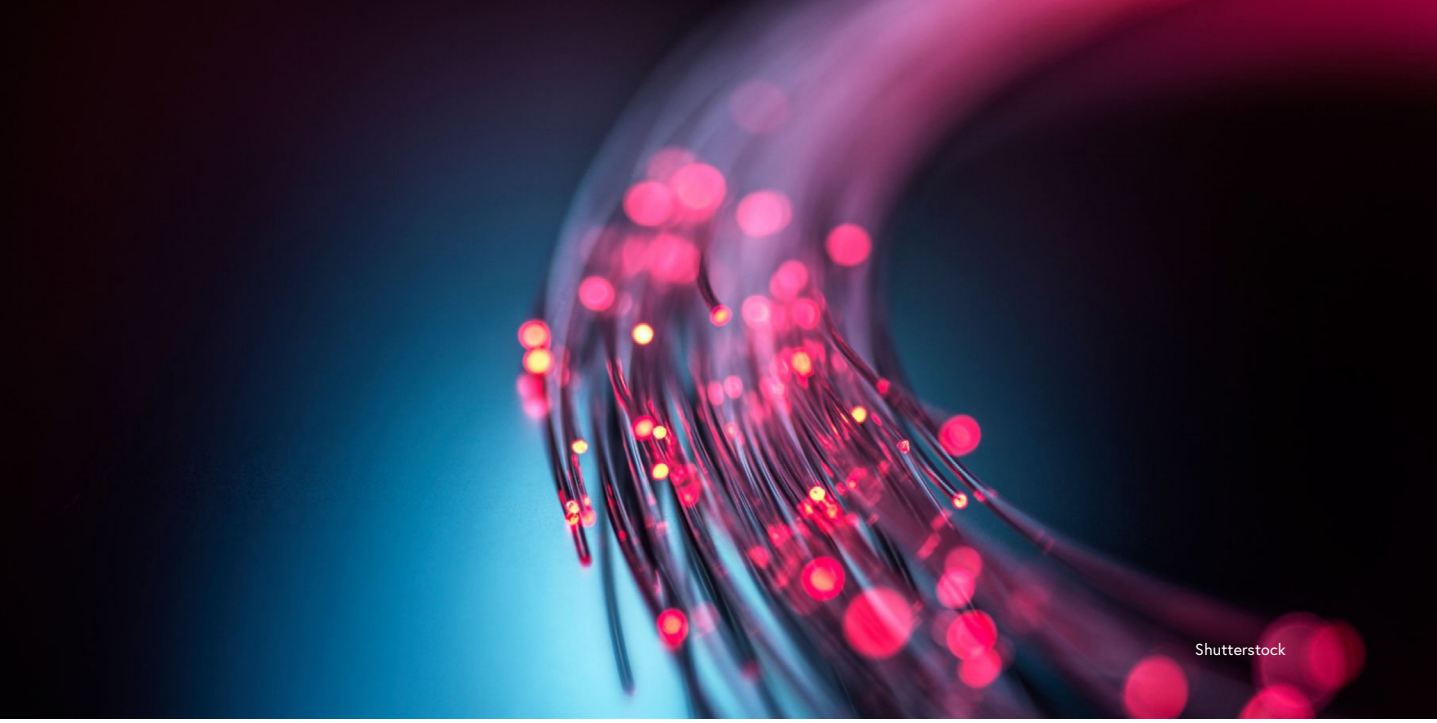
Mag. Alexandra Duca, LL.B ist in der Abteilung Internationales Recht des BMLV mit Arbeitsschwerpunkt u.a. völkerrechtliche Beurteilung neuer Technologien, einschließlich KI, tätig.

Daten ausreichend zu überprüfen und sich dann herausstellt, dass das HuVR verletzt wurde.

Unabhängig vom Grad der Mensch-Maschinen-Interaktion eines KI-Systems kann neben dem Kommandanten bzw. der Kommandantin, die in der Regel Angriffe freigeben oder im Falle eines „human-on-the-loop" entscheiden, dass ein Angriff nicht abgebrochen wird, auch menschliche Bedienerinnen und Bediener eines KI-Systems verantwortlich gemacht werden. Ebenso können sich auch Programmiererinnen und Programmierer des Systems sowie jene, die Daten für das KI-System zur Verfügung stellen, auf deren Basis es in weiterer Folge operiert, nicht grundsätzlich der Verantwortung entziehen. Hinter einem KI-Einsatz steckt in der Regel eine komplexe Organisationsstruktur, wobei im Ernstfall feststellbar sein muss, an welcher Stelle etwas schiefgelaufen ist.

Conclusio

Der erste Schritt in der rechtlichen Beurteilung eines KI-Einsatzes im militärischen Bereich stellt demnach die rechtliche Einordnung der Situation dar. Daran sind die anwendbaren Rechtsbestimmungen geknüpft. In Zeiten eines bewaffneten Konflikts schreibt das HuVR als durchaus flexibles Rechtsgebiet eine Reihe von Regeln vor, die oftmals im Einzelfall abgewogen und beurteilt werden müssen. Diese Beurteilungen haben grundsätzlich durch einen Menschen zu erfolgen, wobei eine Zuhilfenahme von KI-Anwendungen möglich ist. Allerdings muss der Einsatz von KI stets eine bewusste Entscheidung des Menschen bleiben und darf selbst kein autonomer Akt sein, um unter anderem die Verantwortungszurechnung im Falle von Rechtsverstößen gewährleisten zu können.


Shutterstock

Künstliche Intelligenz als Gegenstand der Rüstungskontrolle

Das Ringen um die Regulierung einer militärischen Zukunftstechnologie

Die Rüstungskontrolle militärisch genutzter Künstlicher Intelligenz (KI) hat an Dynamik gewonnen, weshalb das Bundesministerium für Landesverteidigung (BMLV) gefordert ist, sich klar zu positionieren.

Michael Retter

Durch die zunehmende Integration von KI erhoffen sich Verteidigungsministerien und Streitkräfte schnellere und bessere Entscheidungen sowie ein bestimmtes Maß an Automatisierung. Die enormen Möglichkeiten, die aus der Anwendung von KI für die militärische Auftragserfüllung resultieren, werden in dieser Broschüre an anderer Stelle ausführlich erläutert. Neben den zahlreichen Chancen ergeben sich aus dieser Entwicklung aber auch mögliche Risiken, insbesondere dann, wenn sich der Nutzen von

KI indirekt oder direkt auf die Gewaltanwendung, also die Herstellung und den Einsatz von Waffen, bezieht. Dabei stellen sich rasch rechtliche, ethische, humanitäre und sicherheitspolitische Fragen wie beispielsweise, ob KI-Systeme eigenständig Kriege auslösen können, KI-gestützte Waffensysteme zu mehr zivilen Opfern führen oder Terroristen durch KI-Anwendungen leichter Zugang zu Waffen erhalten. Sicherheitspolitische Antworten sind hier erforderlich.

Hier kommt die Rüstungskontrolle ins Spiel. Ihr Ziel ist es, durch gezielte Waffenregulierungen zur Wahrung der zwischenstaatlichen Stabilität beizutragen, humanitäres Leid zu verhindern und sicherzustellen, dass sicherheitspolitisch sensible Akteure keinen Zugang zu Waffen erhalten. Die Ergebnisse solcher Rüstungskontrollprozesse sind meist international verhandelte Abkommen.

Was das ganze Unterfangen häufig langwierig, mühsam, ja in Teilbereichen sogar aussichtlos macht, ist der Umstand, dass Staaten bei der Rüstungskontrolle zusammenarbeiten müssen, um Resultate zu erzielen. Das ist vor dem Hintergrund der aktuellen geopolitischen Situation, die von Konflikt, Polarisierung und der Konkurrenz um Zukunftstechnologien geprägt ist, keine einfache Voraussetzung. Aktuelle Rüstungskontrollprozesse zeigen, dass dies jedoch allemal notwendig ist.

Zwischen dem „verantwortungsvollen Einsatz"...

Da die internationale Regulierung ziviler KI-Anwendungen den Bereich „Sicherheit und Verteidigung" entweder explizit oder implizit ausnimmt, entwickelte sich der Rüstungskontrollprozess in klarer Abgrenzung hierzu.

Die erste Initiative in dieser Hinsicht bildete die von den Niederlanden ausgerichtete Konferenz zu „Responsible AI in the Military Domain" („REAIM-Konferenz") im Februar 2023. Als Resultat dieser Veranstaltung nahmen zahlreiche der anwesenden Staaten den sogenannten „Call-to-Action" an. Außerdem kündigten die Niederlande die Einrichtung der „Global Commission on Responsible AI in the Military Domain" an, die von Expertinnen und Experten ausgearbeitete Berichte und Empfehlungen vorlegen und so einen inhaltlich fundierten Beitrag für die internationalen Diskussionen liefern soll.

Für einige Teilnehmerinnen und Teilnehmer überraschend stell-

ten auch die USA im Rahmen der REAIM-Konferenz ihre eigene Initiative vor, die US-Deklaration zu „Responsible Military Use of AI and Autonomy".

Sowohl der „Call-to-Action" als auch die US-Deklaration sind für die Staaten „politisch verbindlich", es handelt sich nicht um völkerrechtliche Verträge. Beide Abkommen drehen sich um den zentralen Begriff des „verantwortungsvollen Einsatzes" militärisch genutzter KI. Dieser soll durch die international verbindliche Festschreibung bestimmter Normen, darunter Prinzipien, Standards und praktische Maßnahmen, erreicht werden. Die Staaten sind somit aufgefordert, diese Normen bei der Integration von KI in die Verteidigungsministerien und Streitkräfte zu berücksichtigen.

Zu den Verdiensten beider Initiativen gehört es, dass sie erstmalig den Fokus auf die möglichen Risiken militärisch genutzter KI richten, sinnvolle Normen zu deren Verringerung aufzeigen und eine Plattform für Dialog und Austausch bereitstellen. Ein Wermutstropfen bleibt aber die begrenzte Beteiligung. Nur rund 60 Staaten weltweit unterstützen jeweils den Call und die Deklaration.

… und der Regulierung Autonomer Waffensysteme

In einem Artikel, der das Thema „KI im Militär" behandelt, kann eine Thematik nicht unerwähnt bleiben: Autonome Waffensysteme (AWS). Dabei handelt es sich um Systeme, die, einmal aktiviert, ohne weiteren menschlichen Eingriff Ziele auswählen und bekämpfen können.

KI wird von Expertinnen und Experten als jene Technologie gesehen, die einen Quantensprung im Bereich der AWS auslösen könnte. Die Rüstungskontrolle agierte hier enorm vorausschauend, da die Staaten bereits seit 2014, also lange vor dem Hype um maschinelles Lernen und generative KI, im Kontext der Konventionellen Waffenkonvention (KWK) über diese Systeme diskutieren. Dabei steht vor allem die Frage im Mittelpunkt, ob der Einsatz von AWS in bewaffneten Konflikten das Humanitäre Völkerrecht bzw. ethische Prinzipien gefährden könnte.

Obwohl sich die KWK frühzeitig mit möglichen Rüstungskontrollregulierungen von AWS beschäftigte, sind Ergebnisse noch ausständig. Das liegt an der Komplexität der Thematik und an den ausgeprägten Interessen der Staaten. Aktuell besteht jedoch die Hoff-

Michael Retter, BA MA, ist in der Abteilung Militärpolitik des BMLV mit Arbeitsschwerpunkt u.a. Rüstungskontrolle neuer Technologien tätig.

nung, dass bis 2026 ein Durchbruch gelingen könnte. Da sämtliche militärisch relevanten Staaten KWK-Mitglieder sind und daher an ein mögliches Abkommen gebunden wären, hätte dieses eine besonders hohe Effektivität.

Um den Rüstungskontrollprozess voranzubringen, verabschiedete die Generalversammlung der Vereinten Nationen 2023 auch erstmalig eine Resolution zu AWS. Die österreichische Diplomatie war daran maßgeblich beteiligt. Somit beschäftigen sich momentan zwei Prozesse im Rahmen der Vereinten Nationen mit der AWS-Thematik: die KWK und die Generalversammlung.

BMLV-Position

Die Rüstungskontrolle militärisch genutzter KI gewinnt, wie dargestellt, an Dynamik.

Das Jahr 2023 markierte in dieser Hinsicht durch die Entstehung neuer und die Ausdifferenzierung bestehender Prozesse einen Wendepunkt.

Für das BMLV wird es daher immer wichtiger, sich in diesem Bereich klar zu positionieren. Für das Ressort gilt dabei die Maxime „Chancen nutzen, Risiken minimieren". Ein wichtiger Bestandteil dieser Ambition ist der „verantwortungsvolle Einsatz" sämtlicher im BMLV oder ÖBH genutzter KI in Übereinstimmung mit rechtlichen Bestimmungen, politischen Vorgaben und ethischen Prinzipien. Mögliche Risiken von KI gilt es frühzeitig zu erkennen, in den Planungen zu berücksichtigen und gezielt zu minimieren. Das betrifft insbesondere die Gewaltanwendung. Im Sinne des „verantwortungsvollen Einsatzes" ist klar, dass diese immer unter menschlicher Kontrolle stattfinden muss.

Künstliche Intelligenz und Automatisierung im Staatswesen

Ein ethischer Ansatz

Das Potenzial in der Automatisierung hoheitlicher Vollzüge wird nur dann angemessen begriffen, wenn zugleich die Frage nach den Grenzen der Automatisierung im Bewusstsein gehalten wird.

Max Gottschlich

Der Ausdruck „künstliche Intelligenz“ (KI) ist irreführend. Eine Maschine ist kein Selbst, das fühlt, wahrnimmt, vorstellt, urteilt und schließt. Es ist sinnlos, in Bezug auf Maschinen von Handlung, Schuld, Zurechenbarkeit und Verantwortung zu sprechen. Auch die Rede von „autonomen“ Maschinen ist irreführend. Maschinen sind nicht autonom im Sinne der Selbstbestimmung, sondern sie funktionieren gemäß ihrer Programmierung so, dass sie in einer für uns nützlichen Weise ohne Steuerungsbedarf mit Objekten interagieren. Die KI ist ein System, das Daten in einer durch Algorithmen geregelten Weise zueinander ins Verhältnis setzt. Zeichen

werden gemäß einer errechneten Wahrscheinlichkeit – ohne Bewusstsein ihrer Bedeutung – verknüpft. Dennoch entsteht der Schein verstehenden, folgerichtigen Denkens. Damit haben wir einen Assistenten geschaffen, der durch „automatisiertes Denken" die Datenmassen organisiert. Passender wäre es, von algorithmischen Systemen oder Assistenzsystemen zu sprechen.

Zwei Arten von Maschinen sind zu unterscheiden: Eine, die ihre Funktion nur unter menschlicher Steuerung ausübt, und eine, der Automat, der ohne stetigen Eingriff operiert. Die Exekution der im Programm vergegenständlichten Befehle generiert den Schein von Selbsttätigkeit. Im Begriff des Automaten ist weiter zu unterscheiden zwischen solchen, in denen das automatisierte Denken und die auslagerbare Weltauseinandersetzung linear und starr in den programmierten Bahnen verlaufen, und einer Form von automatisiertem Denken, dessen Hardware und Software eine Beweglichkeit und Wechselwirkungsfähigkeit ermöglichen. Dadurch gewinnt der Automat die Potenz, als Assistenzsystem die Weltauseinandersetzung unter Nützlichkeitsaspekten zu begleiten. Ein Assistenzsystem ist ein Werkzeug, das nicht nur zur physischen Entlastung dient, sondern so potent geworden ist, dass es den Vollzug der Weltauseinandersetzung unterstützen kann – im Begreifen, Urteilen und Schließen sowie im Entscheiden und Handeln.

Innerhalb des Assistenzsystems ist eine Differenz relevant, die in den Ausdrücken „smart" und „intelligent" steckt. „Smart" bezieht sich auf das Finden und Gebrauchen geeigneter Mittel für vorausgesetzte Zwecke, um Lösungen für Probleme zu generieren sowie zu prüfen. Die KI ist darüber hinaus der „intelligente" Assistent, der zum scheinbar selbständigen Agenten wird. Zwei Arten dieses „autonomen" Assistenten sind zu unterscheiden: eine auf ein bestimmtes Gebiet beschränkte Artificial Narrow Intelligence und eine Artificial General Intelligence, in der die KI die Gebiete verknüpft. Möglich wird dies durch ein künstliches neuronales Netz. Eine Verarbeitungsschicht empfängt aktivierende Signale durch eine Eingabeschicht. Das Resultat der Verarbeitung zeigt die Ausgabeschicht.

Im Unterschied zum Schaltkreis erlaubt das neuronale Netz eine Plastizität der Funktionalität im Gebrauch. Einerseits sollen sich im neuronalen Netz gemäß den Regeln des Algorithmus Gewichtungen bestimmter Verknüpfungen herauskristallisieren, die

ein „Erkennen“ von komplexen Mustern ermöglicht; andererseits muss diese Gewichtung plastisch bleiben, um adaptierbar zu sein. Das ermöglicht maschinelles „Lernen“. An dieser Plastizität hängt der Schein der Reflexivität. Durch den Gebrauch des Algorithmus etablieren sich im Substrat des neuronalen Gefüges Verknüpfungen, die zur Grundlage rekalibrierender Veränderung herabgesetzt werden. Die Zweckmäßigkeit des Verfahrens in der Plastizität des Relationierungsprozesses von Daten beruht also auf der in der Natur präsenten Zweckförmigkeit der neuronalen Vermittlung. Die „Intelligenz“ der KI beruht auf dem Prinzip der Nachahmung der Natur durch Technik. Die moderne Bionik greift den in die Antike zurückgehenden Gedanken auf, dass die Kunst die Natur, indem sie diese nachahmt, zur Perfektion bringt. Diese Vorstellung ist in der Entwicklung der KI leitend.

Nutzen

Im Namen der Digitalisierung werden in Bezug auf die Natur und die soziale Welt Datenmassen generiert, die eine Übersetzung des Wirklichen in immer umfassendere, genauere und anpassungsfähigere Modelle ermöglichen. In einem Modell wird die Wirklichkeit in ein System eindeutig bestimmbarer gegenständlicher Relationen zwischen Erscheinungen verwandelt. Was solcherart in die festen Formen eines Modells eingefügt wurde, wird in seinem Verhalten bestimmbar und damit beherrschbar. Je umfassender und genauer die Modelle, desto mehr steigt der Bedarf an automatischen Assistenten, ohne welche die Nutzung der Datenmassen in der Verwaltung der technischen Zivilisation unmöglich wäre. Solche „Erntemaschinen“ bereiten mittels algorithmischer Regeln die Daten nach Nutzenaspekten auf. Dadurch wird es möglich, die Effizienz von Verfahren zu maximieren.

Algorithmische Entscheidungssysteme werden seit den 1980er-Jahren von Banken und Versicherungen genutzt, um die gegebenen Daten in Bezug auf Kreditvergaben und Versicherungspolizzen nach Regeln mathematischer Modelle zur Beurteilung aufzubereiten. Seit den 2000er-Jahren inkludieren diese Systeme maschinelles Lernen. Das ermöglichte ein Operieren mit großen Datenmengen in einer Vielzahl von Bereichen. Je potenter und komplexer Entscheidungssysteme sind, desto schwieriger wird die Nachvollziehbarkeit der Wege und Resultate. So mussten ergänzende Systeme entwickelt werden, die die Entscheidungssysteme erklären – die Erklärbarkeitstechnologien.

Die staatliche Verwaltung hat es wesentlich mit regelbasierten Prozessen zu tun, weshalb die Nutzung von KI naheliegt. Im Gebrauch ist vor allem die Artificial Narrow Intelligence im Vordergrund (Chatbots, Antragsstellung, Datenerfassung, usw.) sowie im Hintergrund (Sachbearbeitung, Ordnung und Klassifizierung von Dokumenten, Workflowmanagement, prädiktive Modellierungen von Ausgaben, usw.). Anwendungen im juristischen Bereich machen es möglich, Sachverhalte zur Masse bisher dokumentierter Fälle und Entscheidungen ins Verhältnis zu setzen. In Anbetracht potenter werdender Systeme stellt sich die Frage nach den Grenzen und objektiven Rückwirkungen dieser Technologie.

Probleme

Die KI entfaltet ihre Funktionalität auf Grundlage bestimmter Voraussetzungen, die die Resultate mitbestimmen. Das betrifft die Auswahl des Datenmaterials, die Form der Verarbeitung im Algorithmus und den Modus des „Trainings“ durch Korrekturen.
Da es im öffentlichen Dienst um die Organisation der Mittel zum Zweck des Gemeinwohls und der Selbsterhaltung des Staates als einer Freiheitswelt geht, muss ein Einsatz solcher Systeme zur Unterstützung der Verwaltung unter der Prämisse maximaler Transparenz erfolgen. Die Verwaltung wie die Politik müssen sich zu den Resultaten dieser Assistenzsysteme ins Verhältnis setzen können. Nur wenn man den Resultaten von Assistenzsystemen nicht blind vertrauen muss, können sie ihrer Bestimmung entsprechen. Das Problem der wachsenden Abhängigkeit staatlicher Akteure von Big Tech und deren Partikularinteressen tangiert bereits eine grundsätzlichere Ebene. Denn damit wird das Vertrauen in den Staat als institutionalisiertem Willen zum Gemeinwohl prekär.

Zur tieferen Problemebene führt die Frage: In welchem Maß ist eine Automatisierung der Vollzüge in der Verwaltung und Gestaltung des politischen Gemeinwesens erstrebenswert? Zunächst ist zu bedenken, dass die Automatisierung auch zu neuen Abhängigkeiten und einem Fähigkeitsverlust führt. Kein up-skilling ohne de-skilling. Dem muss gezielt entgegengewirkt werden. Die Automatisierung schlägt darüber hinaus auf das Selbstverständnis von Recht und Staat zurück. Je mehr hoheitliches Handeln auf Assistenzsysteme ausgelagert wird, desto mehr entfremdet sich der Staat von seiner Bestimmung. Der Staat ist keine Maschine, keine Technokratie, in der Bürger wie Datensätze

verwaltet werden, sondern eine organische Einheit von Institutionen, in denen den Bürgerinnen und Bürgern gelebte Freiheit begegnen muss, wenn diese den Staat anerkennen sollen. Würde etwa die Rechtspflege automatisiert werden, Angeklagte ihre Urteile von Maschinen, also von Sachen empfangen, so würde dies das Recht der Person, als Nicht-Sache, als Präsenz von Freiheit anerkannt zu werden, verletzen. Die Grenze der Assistenzsysteme besteht darin, dass kein Algorithmus Abwägungen ersetzen kann, die aus dem Wissen und Wollen eines Gemeinwohls, dem Guten und Gerechten für die politische Gemeinschaft entspringen. Ein richterliches Urteil ist schon deshalb nicht eine automatisierbare Subsumtion eines „Falles" unter einer Regel, weil es eine Forderung der Gerechtigkeit ist, die jeweilige Situation im Sinne der Billigkeit zu berücksichtigen.

Hier lauert also eine Falle: Gerade indem sich die Staatsverwaltung durch den Gebrauch der KI perfektionieren will, kann dies existenzbedrohend werden. Denn der Staat hat seine Existenz im Bewusstsein seiner Bürgerinnen und Bürger, die ihn als Ort ihrer Freiheit anerkennen. Lebt die Bevölkerung im Bewusstsein, von einer Technokratie reguliert zu werden, kann sie den Staat nur als äußere Gewalt ansehen, in der sie sich nicht mehr findet. Nur wer sich diese grundsätzliche Problematik vor Augen hält, kann der Gefahr entgehen, dass sich das Mittel, wie beim Goethe'schen Zauberlehrling, gegen den Zweck verselbständigt.

Militärische Aspekte

Der Nutzen der Assistenzsysteme für das Militär liegt darin, durch schnelle Verarbeitung großer Datenmengen aus unterschiedlichen Quellen möglichst umfassend relevante Faktoren ins Kalkül ziehen zu können. Damit soll eine belastbare Grundlage für die laufend nötigen Entscheidungen im Feld generiert werden, was in der komplexen Wechselwirkungsdynamik mit dem Feind den eigenen Vorteil sichern soll. Dabei geht es um den Faktor Zeit, die Präzision und Anpassungsfähigkeit der Streitkräfte auf allen Ebenen. Analysetools sollen das Geflecht des Geschehens modellieren und überblickbar machen, bis hin zur Antizipation künftiger Szenarien. Darüber hinaus verspricht man sich, die Abhängigkeit von „menschlichen Faktoren" in der Einschätzung der Lage reduzieren zu können.

Doch nachdem auch „systemische Konkurrenten" Assistenzsysteme einsetzen, entsteht eine Dyna-

DDr. Max Gottschlich ist am Institut für Praktische Philosophie/Ethik der KU Linz tätig.

mik der Automatisierung in der militärischen Rüstung, in der es – gleich dem KI-gestützten Aktienhandel – auch um einen Wettlauf um den Faktor Zeit geht. Aus der Angst vor dem gegnerischen Vorteil entsteht ein Drang zur Integration von KI in Militärtechnologie. Die Argumente für die Nützlichkeit der Militärrobotik für die Aufklärung und Präzisionsangriffe liegen auf der Hand. Die Risikominimierung für die eigenen Soldatinnen und Soldaten sowie die Reduktion von Kollateralschäden durch maschinelle Präzision werden auch als ethisch relevante Argumente für deren Einsatz ins Treffen geführt.

Die Probleme liegen auf der Hand: Die technische Ebene betrifft vor allem die Fehleranfälligkeit in der Unterscheidung von Freund und Feind durch Algorithmen sowie eine wachsende empfindliche Abhängigkeit der Funktionalität des Militärs von der Funktionalität von Systemen, den Herstellern und erforderlichen Ressourcen.

In der Logik von Assistenzsystemen liegt es, dass sie durch den Modus ihrer Aufbereitung des Datenmaterials implizit Entscheidungen nach Nützlichkeitsgesichtspunkten nahelegen. Je höher die Potenz der Systeme, je abhängiger der Mensch wird, desto höher erscheint der Grad der Verbindlichkeit dieser Handlungsempfehlungen. Die Automatisierung umfasst dann indirekt auch die Entscheidungen selbst.

Die wachsende Automatisierung der Kriegführung generiert eine beschleunigende und enthemmend-dehumanisierende Dynamik. Alle hemmenden Faktoren im Kriegsgeschehen, auf die Clausewitz hinwies, hängen an einer hinterfragenden Reflexion des tödlichen Wechselwirkungsgeschehens. Solche Hemmung entfällt beim Automaten. Dies unterstreicht die Dringlichkeit der Aufgabe für die internationale Gemeinschaft, sich zu einer rechtlichen Einhegung des militärischen Einsatzes der KI im Sinne des Humanitären Völkerrechts durchzuringen.

Shutterstock

Künstliche Intelligenz im geopolitischen Machtkampf

KI ist eine emergente und disruptive Technologie, die alle Aspekte der Gesellschaft berührt. Kontrolle über diesen Technologiebereich beinhaltet somit ein massives Potenzial zur wirtschaftlichen und militärischen Machtprojektion. In dem daraus resultierenden geopolitischen Wettstreit stehen sich zwei Seiten gegenüber: einerseits die demokratische und andererseits die autokratische.

Daniel Hikes-Wurm

Der geopolitische Wettstreit zwischen dem demokratischen Modell des „Westens“ und dem machtzentrierten und autokratischen Modell Chinas, unterstützt durch gleichgesinnte Staaten wie Russland und den Iran, beinhaltet auch eine technologische Komponente. Das betrifft sowohl die Kontrolle über die eigentliche Technologie als auch über die Regeln zu deren Anwendung. Die sektorenübergreifende Natur von KI und deren inhärenter Dual-Use-Charakter verstärken außerdem das Verschwimmen traditionaler Grenzen zwischen Staat und Gesellschaft.

Kontrolle über die Technologie

Sowohl China als auch die USA ringen seit Jahren um die Vorherrschaft über KI, sowohl zur Machtausübung in Wirtschaft als auch nationaler Sicherheit. Hierbei haben beide Seiten technologische Vorsprünge erzielt, die sie der jeweils anderen Seite vorenthalten wollen.

China nimmt sowohl quantitativ als auch qualitativ eine Spitzenposition in der Entwicklung von Patenten zu KI ein, und rund die Hälfte der weltweit führenden/anerkanntesten KI-Forscherinnen und Forscher kommen aus China. Die chinesische Staatsführung ist durch strenge Kontrollen von Forschung und Entwicklung sowie geistigem Eigentum bestrebt, dieses Know-how im Inland zu halten. Chinas Zugang zu Datensicherheit und Privatsphäre lässt chinesischen Unternehmen außerdem mehr Spielraum als westlichen Unternehmen beim Training von KI-Modellen, vor allem in Bereichen die in den USA und Europa als besonders sensibel gelten, wie beispielsweise Überwachung.

China hinkt dafür weiterhin vor allem bei der Hardware hinterher. Westlich orientierte Unternehmen arbeiten in globalen Lieferketten zusammen, wie beispielsweise NVidia (USA) für Design, ASML (Niederlande) für Produktionsanlagen und TSMC (Taiwan) für die Fertigung. Aufgrund von US-bestimmten Exportkontrollen ist China weitgehend von diesen Lieferketten ausgeschlossen. Auch im Bereich wirtschaftlich erfolgreicher Anwendungen wie Sprachmodellen sind Unternehmen aus den USA, inklusive OpenAI, Meta und Google, weiterhin weltweit führend. Europäische KI-Unternehmen, die oftmals in Nischenbereichen erfolgreich sind, fehlen indes weiterhin an der globalen Spitze. Mit dem AI Act als erste umfangreiche Gesetzgebung zu KI-Modellen versucht die EU nun, die eigene Machtposition aufzubauen.

Kontrolle über Normen und Standards

Das rasante Voranschreiten dieser gesellschaftsübergreifenden Technologie wirft weitreichende ethische Fragen auf, vor allem in Bereichen, in denen bestehende Standards und Regulierungen nicht ausreichen. Auch hier gibt es ein geopolitisches Mächteringen um die Kontrolle darüber, was erlaubt und was eingeschränkt werden soll. Hier treffen auf der einen Seite das demokratische, wertebasierte System des „Westens“ und auf der anderen das

autokratische und machtzentrierte System Chinas aufeinander.

Im Westen – also die USA, Europa, aber auch gleichgesinnte Staaten wie Südkorea, Japan und Australien – werden Rechte zur Meinungsfreiheit, Privatsphäre und Menschenrechte als übergeordnet und unverletzbar erachtet. Um diese zu sichern, bedarf es strikter Auflagen zur Verwendung persönlicher Daten und einen risikobasierten Ansatz für KI-Modelle, wie er beispielsweise im AI Act angestrebt wird. Gleichzeitig werden eine gewisse Offenheit und Transparenz von KI-Modellen vorausgesetzt, um den Schutz demokratischer Werte zu gewährleisten. Diesen Werten haben sich grundsätzlich alle Staaten und Unternehmen unterzuordnen, obgleich es innerhalb dieser „westlichen" Gruppierung natürlich auch gewisse Auslegungsunterschiede gibt (z.B. zwischen USA und EU).

Dem gegenüber steht das chinesische Modell, das auf staatliche Vorgaben ausgelegt ist. Für China hat technologische Souveränität oberste Priorität. Dies geht mit einem sehr engen Souveränitätsverständnis und der Skepsis gegenüber supranationalen Verpflichtungen, die aus chinesischer Sicht stark westlich geprägt sind, einher. Datenschutz hat in China zwar einen besonderen Stellenwert, jedoch nur insoweit, dass Daten das Land nicht verlassen dürfen. Im Inland dürfen auch persönliche Daten sehr viel umfangreicher eingesetzt werden im Vergleich zu den USA oder der EU. Implizit beinhaltet dies eine gewisse Verschlossenheit von KI, denn somit obliegt die Festlegung und die kurzfristige Abänderung der Spielregeln jedem Staat selbst. Zudem entfällt die demokratische Anforderung, dass KI-Systeme gegenüber der Bevölkerung transparent sein müssen – stattdessen wird größere Rechenschaftspflicht gegenüber dem Staat selbst verlangt.

Die schleichende Militarisierung der Gesellschaft

Durch die zunehmende Vernetzung der Gesellschaft und den grenzüberschreitenden Charakter des Internets werden Konflikte immer stärker Teil des zivilgesellschaftlichen Alltags. Dies betrifft nicht nur die Berichterstattung, wodurch Konflikte in Echtzeit weltweit mitverfolgt werden können, sondern auch wie die Zivilgesellschaft und die Privatwirtschaft mit Konflikten interagieren. Privatunternehmen sind bereits ein wichtiger Bestandteil von Kriegen. Prominente Beispiele hierfür sind das Mitwirken von Microsoft und

Starlink im Krieg in der Ukraine, sowie der weitgehende Einsatz von Drohnen des zivilen Markts der chinesischen Firma DJI.

Darüber hinaus sind in den USA Kooperationen mit privatwirtschaftlichen Technologieunternehmen aus „Silicon Valley" bereits ein wesentlicher Teil der digitalen Transformation der Streitkräfte. Auch in der EU wurde mittlerweile das gesellschaftliche Tabu der zivil-militärischen Zusammenarbeit durchbrochen. Das milliardenschwere EU-Forschungsförderprogramm „Horizon Europe" unlängst auch für Dual-Use-Anwendungen geöffnet. Somit wird die nationale Sicherheit und Verteidigung nicht mehr ausgeschlossen.

Die Verschmelzung von staatlicher Sicherheit mit der Zivilgesellschaft ist in China im Rahmen des Konzepts der zivil-militärischen Fusion noch wesentlich expliziter ausgeprägt. Hierbei ist auch rechtlich vorgeschrieben, dass Unternehmen und Forschungsinstitutionen aller Art ihre Innovationen mit dem Staat teilen müssen, sofern diese als für die nationale Sicherheit relevant eingestuft werden. Das kann jederzeit und ohne Vorankündigung passieren. Dies betrifft auch sämtliche Daten, die innerhalb Chinas gespeichert und der Führung zugänglich gemacht werden müssen.

Dieses schrittweise Verschwimmen von zivilen und militärischen Grenzen geht jedoch weit über staatlich kontrollierte Aspekte hinaus. Jede Person mit Internetzugang ist mittlerweile dazu befähigt, in Konflikte einzugreifen. So haben beispielsweise tausende Privatpersonen aus ganz Europa durch Fundraising-Spenden zum Ankauf von Munition und Waffen oder der Teilnahme an umfangreichen Cyber-Kampagnen gegen Russland, die Ukraine unterstützt. Dies wirft die Frage auf, ob solche Privatpersonen, die sich freiwillig über das Internet an Konflikten beteiligen, unter dem bestehenden humanitären Völkerrecht noch als Zivilistinnen und Zivilisten zu betrachten sind. Das gleiche gilt natürlich für Unternehmen, die eine zunehmend aktive Rolle in Konflikten spielen. Für geopolitische Akteure bedeutet all dies außerdem, dass die Kontrolle über strategische Unternehmen und die Einflussnahme auf die Zivilgesellschaft zunehmend an Bedeutung gewinnen.

Der geopolitische Wettstreit schreitet voran

Die Vor- und Nachteile strikter Regulierungen müssen abgewogen werden. Dies betrifft vor allem Europa. Die EU sieht sich zwar nach wie vor als Normierungssupermacht, da in Brüssel verabschiedete Vorgaben (z.B. DSGVO) weltweit beachtet werden, aber dieser „Brüssel-Effekt" kann untergraben werden, wenn Vorschriften wirtschaftlichen Schaden anrichten. Ob dies beim AI Act und derart strikten Vorgaben der Fall sein wird, bleibt abzuwarten.

Obgleich Chinas Ansatz zunächst effizienter erscheinen mag, weist es jedoch einige, nicht von der Hand zu weisende Nachteile auf. Ein Grund weswegen chinesische Sprachmodelle in puncto Leistungsfähigkeit hinter den US-amerikanischen zurückbleiben ist die Tatsache, dass sich chinesische Modelle strikt an staatliche Vorgaben halten müssen und somit auch nicht alles wiedergeben dürfen, was verwendete Daten ermöglichen würden.

Eine zunehmende Trennung beider Einfluss-Sphären findet wahrscheinlich, nicht nur aufgrund des unterschiedlichen Werte-Ansatzes, sondern auch wegen dem gegenseitigen Bestreben der wirtschaftlichen Entkoppelung statt. Ob „de-coupling" in den USA, „de-risking" in Europa oder die „securitization" in China, alle geopolitischen Akteure wollen ihre Wirtschaft und Gesellschaft derzeit von übermäßiger Einflussnahme der jeweils Anderen schützen.

Die EU, die im Namen der strategischen Autonomie eine Diversifizierung der Lieferketten anstrebt, hat hiermit jedoch auch die USA im Visier. Transatlantische Zusammenarbeit bleibt dennoch notwendig, um den demokratischen/westlichen Regulierungsansatz durchzusetzen. Hierfür wurde bereits der „EU-US Trade and Technology Council" (TTC) ins Leben gerufen. Die USA sehen eine besondere, sicherheitspolitische Aufgabe für den TTC, während Brüssel darin immer noch vor allem ein Instrument der wirtschaftlichen Kooperation sieht. Eine engere sicherheitspolitische Kooperation ist jedoch unabdinglich, vor allem wenn die EU bei Sanktionen und Exportkontrollen der USA mitentscheiden möchte.

China setzt indessen schon seit Jahren Sanktionen und andere wirtschaftliche und gesellschaftliche Druckmittel ein, um nationale Ziele zu erreichen. Beispiele hierfür beinhalten die

Oberst Daniel Hikes-Wurm ist in der Generaldirektion Verteidigungspolitik des BMLV mit Arbeitsschwerpunkt hybride Bedrohungen und neue Technologien tätig.

Seltene-Erden-Sanktionen gegen Japan (2010), den Konsumboykott gegen Südkorea (2016), den Import-Stopp gegen litauische Produkte, nachdem Taiwan dort ein Repräsentationsbüro eröffnet hatte (2021) sowie die Sanktionen gegen australische Export-Industrien nachdem der australische Premierminister zur unabhängigen Untersuchung des COVID-19-Ausbruchs in Wuhan aufrief (2020). Neue Technologien, inklusive KI und anderer strategischer Technologien, können in Zukunft als zusätzliches Druckmittel dienen.

Abschließend stellt sich die Frage der Deutungshoheit des westlichen Ansatzes. Während der westliche Ansatz als selbstverständlich gilt, sind die meisten anderen Staaten nicht davon überzeugt. Es herrscht weiterhin ein Ringen um Einfluss über Länder des globalen Südens, von denen viele die Legitimität und Übertragbarkeit des westlichen Ansatzes hinterfragen.

China bietet vielen Entwicklungsstaaten Möglichkeiten, denen Europa und die USA nur beschränkt entgegenwirken können. Ein Beispiel hierfür ist der 5G-Ausbau in Afrika, der fast ausschließlich von chinesischen Unternehmen wie Huawei durchgeführt wurde.

Während westliche Regierungen vor der Zusammenarbeit mit China warnten, aber keine Alternativen anboten, stellten chinesische Unternehmen umfangreiche Gesamtlösungen, inklusive Aufbau und Betrieb von Telekommunikationsinfrastruktur, zu erschwinglichen Preisen bereit. Wenn, in Bezug auf KI, technologische Gesamtlösungen zu leistbaren Preisen angeboten werden, und diese außerdem schon mit integrierten Lösungsansätzen eine bessere Überwachung und Kontrolle von Staat und Gesellschaft beinhalten, dann werden westliche Warnungen und das Bemühen um einen genuin „menschenzentrierten“ Ansatz voraussichtlich zu wenig Attraktivität ausstrahlen.


Shutterstock

Künstliche Intelligenz und ihre Rolle in aktuellen Konflikten

Zu Beginn des 21. Jahrhunderts hat sich das bis dahin gewohnte Konfliktmuster grundlegend verändert – von der asymmetrischen über die hybride bis zur konventionellen Kriegführung auf hohem Niveau. Hinzu kommen technologische Entwicklungen, deren Auswirkungen weitaus einschneidender sind und deren volles Ausmaß noch nicht abgeschätzt werden kann. Die Digitalisierung, inklusive der Entwicklung leistungsfähiger Informationstechnologien und Künstlicher Intelligenz (KI), schufen die Voraussetzungen für eine neue Revolution der Kriegführung.

Markus Reisner

Ein entscheidender Entwicklungsschritt im Bereich der militärischen Landesverteidigung wurde durch die Automatisierung und Autonomisierung militärischer Aufklärungs-, Waffen, Führungsinformations- und Zielfindungssysteme erreicht. Das Militär verschiedener Staaten erkannte die sich bietenden Möglichkeiten frühzeitig und versuchte, Verfahren und Taktiken weiterzuentwickeln. Testserien wie die „AlphaDogfight Trials“ 2018, virtuelle Luftkämpfe zwi-

schen Menschen und Maschine der US-amerikanischen Behörde für fortgeschrittene Verteidigungsforschungsprojekte (DARPA), die britischen „Storm-Cloud"-Versuche 2021 (domänenübergreifender Einsatz in einem transparenten Gefechtsfeld) und reale Einsätze wie das US-Projekt „Maven" in Afghanistan 2017 (automatische Verfolgung von menschlichen Zielpersonen) waren sowohl Blaupause als auch Vorgeschmack.

Wirkung auf dem aktuellen Gefechtsfeld

Aktuelle Kriege, beispielsweise der russische Angriffskrieg gegen die Ukraine, aber auch der Gaza-Krieg, lassen Fiktion nun zunehmend Wirklichkeit werden. Es lassen sich bereits jetzt zwei wesentliche Einsatzmöglichkeiten für KI erkennen: Einerseits der Einsatz von Aufklärungs- und Waffensystemen in den unterschiedlichen Domänen der Kriegführung und andererseits die Unterstützung der Beschleunigung militärischer Entscheidungen in Führungsinformations- und Zielfindungsprozessen. Der Einsatz unbemannter, halbautonomer, roboterähnlicher Aufklärungs- und Waffensysteme eröffnet den beteiligten Streitkräften bisher ungeahnte domänenübergreifende Möglichkeiten und die Prozessbeschleunigung beeinflusst die Schnelligkeit der eigenen Waffenwirkung.

In der Ukraine führt der Einsatz von zehntausenden Drohnen gleichzeitig und auf beiden Seiten zu einem transparenten Gefechtsfeld. Es ist kein unerkanntes Bereitstellen von Kräften mehr möglich. Jedes Manöver bleibt im Hagel von Kamikazedrohnen und schnell feuernder Artillerie liegen. Gleichzeitig liefern diese Drohnen Daten, die durch KI-basierte Software analysiert werden. Ziele werden somit rasch erkannt und ohne Zeitverzug bekämpft. Ein Beispiel hierfür ist die ukrainische GIS-ARTA-Software, die Daten über russische Ziele für eigene Artilleriebatterien sammelt.

Andere Beispiele zeigen auf, welche Anwendungsbereiche von KI bereits jetzt möglich sind. Im Frühjahr 2024 tauchte in der Ukraine ein erstes Video auf, in dem ein russischer Angriff unter dem Einsatz von Bodenrobotern auf einen ukrainischen Infanteriestützpunkt durch den Einsatz von „First-Person-View"-Drohnen abgewehrt wurde. Inzwischen unterstützt die US-Armee die ukrainischen Streitkräfte mit Algorithmen, um vorherzusagen, wann ukrainische Haubitzen neue Läufe benötigen. Zeitgleich entwickeln Russland und die Ukraine Software, um

Drohnen in die Lage zu versetzen, zu einem Ziel zu navigieren und ein Ziel autonom ansteuern zu können, selbst wenn Störsender die Verbindung zwischen Pilotinnen und Piloten und Drohnen unterbrechen. Schließlich wurde im Zusammenhang mit dem Gaza-Krieg im April 2024 bekannt, dass die israelischen Verteidigungskräfte (IDF) ein als „Lavender" bekanntes KI-Tool nützen, um unter tausenden Palästinenserinnen und Palästinensern mutmaßliche Hamas-Terroristen zu identifizieren.

Neue Rahmenbedingungen

Die Grenzen von Raum und Zeit haben sich durch diese KI-gestützten Entwicklungen für militärische Operationen verändert. Die bisher bekannten Parameter für militärisches operatives Denken, nämlich Kraft, Raum, Zeit und Information, beginnen sich zu verändern. Hierdurch ergeben sich neue Möglichkeiten für die Streitkräfte, aber auch Anpassungsbedarf an geänderte Rahmenbedingungen. Die menschliche Kontrolle über bemannte und unbemannte Waffensysteme und militärische Software in Führungsinformationssystemen wird über Netzwerkstrukturen im Cyber-Raum oder im elektromagnetischen Feld ausgeübt. Für den Fall, dass es einem Gegner gelingen sollte, die eigenen Netzwerke zu kontrollieren und zu durchdringen, müssen optionale Angriffs- oder Verteidigungsstrategien existieren.

Aufgrund der eingeschränkten Kommunikation können diese Strategien nur auf einem höheren Grad an Autonomie von Soft- und Hardware beruhen. Gerade in der Domäne Cyber wird daher die Entwicklung von teilautonomen KI-Programmen aktiv vorangetrieben. Ein Beispiel ist die Entwicklung eines Programms namens „Monster Mind" für die US National Security Agency (NSA). Ziel dieses Programms ist es, mögliche Cyber-Angriffe auf die USA frühzeitig zu erkennen und zu neutralisieren. Aufgrund der hohen Geschwindigkeit, mit der solche Operationen durchgeführt werden, ist es das Ziel, das Programm in einem völlig autonomen Modus einzusetzen. Es gibt auch Überlegungen, KI bei der Entscheidungsfindung im Nuklearbereich einzusetzen. Derartige Überlegungen existieren bereits seit Langem: so arbeitete die Sowjetunion bereits während des Kalten Krieges an einem sogenannten „Tote-Hand"-Konzept im Rahmen ihres „Perimeter"-Systems. Dadurch sollte in jedem Fall ein nuklearer Gegenschlag ermöglicht werden.

Zukunftspotenzial

Längerfristig ist davon auszugehen, dass am Ende eines entsprechenden Entwicklungsprozesses vollautonome Aufklärungs- und Waffensysteme sowie Führungsinformations- und Zielauswahlsysteme mit geringer KI in der Lage sein werden, Situationen mittlerer Komplexität selbstständig zu lösen. Hierzu gehören zum Beispiel unbewaffnete Aufklärung, bewaffnete Patrouillen, begrenzte Angriffe in einem definierten und ausgewiesenen Gebiet und Erstzielauswahl durch Datenanalyse.

Teilautonome, mit KI ausgestattete Roboter werden künftig in der Lage sein, mit Hilfe von Sensoren selbstständig Informationen über ihre Umgebung zu sammeln. Diese Informationen werden von Hochleistungsprozessoren verarbeitet und bilden die Grundlage für eine Entscheidung, die dann mittels eingebauter Komponenten (wie Bewegungsmechanismen oder Waffen) umgesetzt wird. Mit zunehmender Erfahrung ist der Roboter immer besser in der Lage, sich selbst zu optimieren und effektiver zu werden. Der Mensch ist auf eine überwachende Rolle reduziert.

Die derzeitigen Ereignisse in Kriegsgebieten machen bewusst, dass unbemannte Aufklärungs- und Waffensysteme sowie KI-unterstützte Führungsinformations- und Zielauswahlsysteme zum Standard in der modernen Kriegführung geworden sind. Der Jahresbericht des Pentagons über die chinesische Militärmacht stellte kürzlich fest, dass die Volksbefreiungsarmee (PLA) damit begonnen hat, über „Multi Domain Precision Warfare“ zu diskutieren. Sie versteht darunter den Einsatz von „Big Data“ und KI zur schnellen Identifizierung wichtiger Schwachstellen in US-Militärsystemen wie Satelliten oder Computernetzwerken. Diese könnten dann angegriffen werden.

Es ist daher davon auszugehen, dass sich die dadurch eingeleitete Transformation der Kriegführung in Zukunft noch weiter beschleunigen wird. Allerdings ist es auch nur eine Frage der Zeit, bis die erste, von terroristischen Gruppen oder von im Hintergrund agierenden staatlichen Akteuren gesteuerte Drohne ein Fußballstadion oder schädliche Software, kritische Infrastruktur ins Visier nimmt.

Schon jetzt eignen sich Drohnen als Waffenträger, sei es durch den Transport von Luft-Boden-Waffen oder durch die Beladung mit Sprengstoff.

Drohnen könnten aber auch zum Einsatz chemischer oder biologischer Waffen verwendet werden. Sollte ein solcher Einsatz in einer KI-gesteuerten Schwarmform erfolgen oder sich Schadsoftware im Cyber-Raum mit hoher Geschwindigkeit ausbreiten, könnten derartige Angriffe katastrophale Folgen haben.

Oberst Mag. Dr. Markus Reisner, PhD, ist Leiter des Instituts für Offiziersausbildung an der Theresianischen Militärakademie. Sein Forschungsschwerpunkt ist der Einsatz unbemannter Waffensysteme.

Shutterstock

Die digitale Transformation in Streitkräften

Ein internationaler Vergleich

Die globale digitale Transformation führt zu neuen Organisationsstrukturen für die Implementierung moderner Technologien, wobei Künstliche Intelligenz (KI) eine wichtige Rolle spielt und darüber hinaus neue militärische Fähigkeiten für eine bruchfreie Wirkungsüberlegenheit in allen Domänen ermöglicht. In diesem Artikel wird anhand von öffentlich zugänglichen Quellen untersucht, wie Staaten digitale Technologien in ihre Streitkräfte integrieren, um ihre Verteidigungsfähigkeiten und operative Effizienz zu modernisieren.

Michael Suker

Vereinigte Staaten

Im Verteidigungsministerium der Vereinigten Staaten (Department of Defense, DoD) sind das 2021 gegründete Chief Digital and Artificial Intelligence Office (CDAO) und das US Cyber Command (USCYBERCOM) für die digitale Transformation verantwortlich. Das CDAO ist aus dem 2018 gegründeten Joint Artificial Intelli-

gence Center (JAIC) entstanden und spielt eine zentrale Rolle bei der Entwicklung und Umsetzung von Strategien, die darauf abzielen, technologische Innovationen zu integrieren und die Effizienz sowie die Entscheidungsfindung innerhalb des DoD zu verbessern. Schwerpunkte sind Datenmanagement, KI, Automatisierung und die Entwicklung robuster und sicherer Netzwerke. Dies umfasst auch die Verantwortung für die Implementierung von Initiativen wie Joint All-Domain Command and Control (JADC2), die darauf abzielen, die Kommando- und Kontrollfähigkeiten über alle militärischen Domänen hinweg zu integrieren und zu optimieren.

Im Gegensatz zur KI-Strategie aus 2018 und der Datenstrategie aus 2020 orientiert sich die im Jahr 2023 veröffentlichten Data, Analytics, and Artificial Intelligence Adoption Strategy an einer KI-Bedarfshierarchie. Diese neue Ausrichtung betont die Bedeutung hochwertiger Daten und zielt darauf ab, schnelle und flexible Anpassungsprozesse, Datenanalysen sowie eine verantwortungsvolle Implementierung von KI sicherzustellen. Aktuell haben diese Organisationen unterschiedliche, aber komplementäre Rollen innerhalb des US-Militärs. Während USCYBERCOM für Cyber-Verteidigung und -Operationen verantwortlich ist, konzentriert sich das CDAO auf die strategische Integration digitaler Technologien mit Schwerpunkt KI, um die Effizienz und Effektivität militärischer und administrativer Prozesse zu verbessern. Mit ihrem Personal stellen die USA damit auch die wesentliche Infrastruktur für das Federated Mission Networking (FMN) der NATO zur Verfügung, das auf der Grundlage der Erfahrungen des Kriegs in Afghanistan gegründet wurde, um die Zusammenarbeit in Joint Operations innerhalb der NATO zu verbessern.

Die USA spielen außerdem eine Schlüsselrolle im Defence Innovation Accelerator for the North Atlantic (DIANA), der 2021 zur Förderung ziviler und militärischer Innovationen und der transatlantischen Zusammenarbeit bei kritischen Technologien gegründet wurde. DIANA unterstützt Unternehmen über ein Netzwerk von über 200 Beschleunigungs- und Testzentren in derzeit 28 von 32 NATO-Mitgliedsstaaten.

Deutschland

Das Zentrum für Digitalisierung der Bundeswehr (ZDigBw) spielt eine Schlüsselrolle bei der Digitalisierung der Bundeswehr. Als Exzellenzzentrum und Treiber für

Digitalisierung ist die Dienststelle dem Kommando Cyber- und Informationsraum (CIR) unterstellt und verspricht aufgrund der Bündelung der Digitalisierungsaufgaben erhöhte Effizienz und kürzere Innovationszyklen. Die Koordinierung sowie die Fähigkeitsentwicklung des militärischen Nachrichtenwesens, der elektronischen Kampfführung, der operativen Kommunikation, des Geoinformationswesens und der Informationssicherheit wird durch das ZDigBw sichergestellt.

Zu den Hauptaufgaben des etwa 800 Mitarbeitenden umfassenden ZDigBw gehören die dimensionsspezifische Entwicklung und Integration neuer Softwareprodukte sowie die Anpassung bestehender kommerzieller und militärischer Softwarelösungen an die Anforderungen der Bundeswehr. Ein Schwerpunkt liegt dabei auf der Harmonisierung der IT-Systeme und der Verbesserung der Interoperabilität innerhalb der NATO durch das FMN. Als eines der Leuchtturmprojekte wird die Einführung eines umfassenden digitalen Informations- und Datenverbunds bis hin zu Führungs- und Waffeneinsatzsystemen durch ein integriertes Battle Management System angeführt.

Frankreich

Frankreich veröffentlichte bereits 2019 die nationale Strategie für „Künstliche Intelligenz zur Unterstützung der Verteidigung“, in der ein langfristiger und holistischer Ansatz zur stufenweisen Einführung von KI in allen Bereichen der Streitkräfte verfolgt wird. Für die strategische Ausrichtung und Umsetzung der digitalen Transformation in der gesamten Struktur des französischen Verteidigungsministeriums ist die interne Generaldirektion für Digitalisierung und Informations- und Kommunikationstechnologie (Direction générale du numérique et des systèmes d’information et de communication, DGNUM) zuständig.

Die Agentur für Digitalisierung in der Verteidigung (Agence du Numérique de Défense, AND) ist die zentrale Stelle für die digitale Transformation innerhalb der DGNUM. Sie wurde 2021 eingerichtet und umfasst etwa 400 Bedienstete. Die AND übernimmt eine Schlüsselrolle bei der Implementierung neuer Technologien und Koordination aller wichtigen digitalen Projekte und sorgt für die Modernisierung der digitalen Infrastruktur der Armee. Die Aufgabenstellungen umfassen die Bündelung vorhandener Kapazitäten und die Koordination von

Ressourcen zur Umsetzung der digitalen Transformation sowie die Beratung anderer Dienststellen innerhalb des Verteidigungsministeriums.

Schweiz

Aufbauend auf der Vision 2030 verfolgt die „Dachstrategie Digitale Transformation“ der Schweizer Armee das Ziel, die Einsatzbereitschaft digitaler Technologien durch KI zu stärken. Kernelement ist die Standardisierung von Daten, was die Integration innerhalb der Streitkräfte und die Integration in nationale und internationale Verbundnetze sicherstellen soll.

Ein Schwerpunkt bildet das Sensor-Nachrichten-Führung-Wirkungssystem (SNFW), das die Integration nach internationalen Standards unterstützt und vorantreibt. Das übergeordnete Ziel des SNFW ist es, diese verschiedenen Elemente nahtlos miteinander zu verbinden und die Grundlagen für eine effektive und effiziente Einsatzführung zu schaffen. Zur Umsetzung der digitalen Transformation wurde das Projekt „Langfristige Entwicklung der Gruppe Verteidigung und Armee“ aufgestellt und das Kommando Einf K/UK TK A als spezielle Einführungsorganisation eingerichtet, das sukzessive in das Kommando Cyber integriert wird. Ein Projekt der Einführungsorganisation ist die Implementierung einer Digitalisierungsplattform, die als Basis für Softwareprodukte dienen wird.

Zusammenfassung und Ausblick

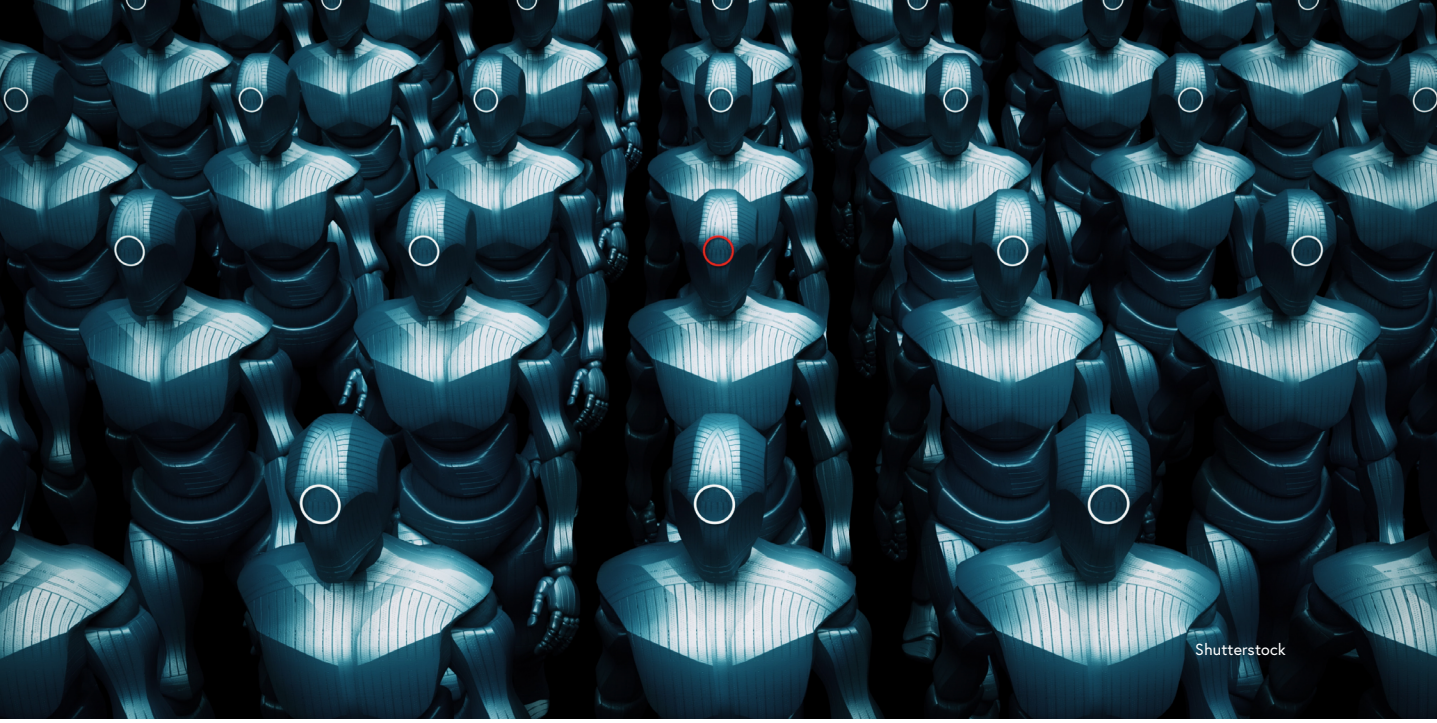
Fortschreitende Automatisierung und der Einsatz technischer Assistenzsysteme in Kombination mit hoher Geschwindigkeit, Präzision und Tödlichkeit prägen moderne bewaffnete Konflikte. Das Potenzial von KI hat zu einem Paradigmenwechsel bei Command and Control (C2)-Systemen geführt, da es die Geschwindigkeit und Effizienz militärischer Operationen deutlich erhöht. Bei der Umsetzung jeder digitalen Transformation müssen kontinulierlich neue Technologien aktiv evaluiert und in alle identifizierten Geschäftsprozesse implementiert werden. Der Vergleich internationaler Vorgehensweisen zeigt, dass speziell zu diesem Zweck geschaffene Einrichtungen die Entwicklung und den Einsatz fortschrittlicher Technologien evaluieren und die Implementierung in den Streitkräften koordinieren. Sowohl die enge Zusammenarbeit zwischen (nationalen und internationalen) militärischen und zivilen Akteuren als

Michael Suker, BSc MSc ist Leiter des Cyber Dokumentations- und Forschungszentrums an der Landesverteidigungsakademie. Seine Schwerpunkte umfassen die Erkennung von Fake News und die automatisierte Informationsbeschaffung.

auch Innovationsökosysteme, die militärische Dienststellen, Forschungseinrichtungen und Rüstungsunternehmen vernetzen, um neue Technologien und Strategien zu entwickeln und die militärische Effizienz zu erhöhen, werden auch in den verschiedenen Ansätzen anderer europäischer Streitkräfte, wie z.B. der Streitkräfte Estlands, stark forciert.

Mit dem militärischen Konzept „Mosaic Warfare" werden teil- oder vollautomatisierte, modulare und kleine, insbesondere unbemannte Systeme im Verbund mit anderen hochautomatisierten Systemen dimensionsübergreifend eingesetzt.

Konzepte des Kampfes mit digitalen Fähigkeiten (unbemannte Luftfahrzeuge, Internet of Battlefield Things (IoBT), smart devices, KI-targeting Systeme und KI gestützte taktische Planung, etc.) sind im Rahmen von Mosaic Warfare den Ansätzen von AirLand-Battle und Multi-Domain-Operationen deutlichen überlegen. Dies erfordert einen grundlegenden Paradigmenwechsel auf der Basis modularer, funktionaler und vernetzter Plattformen.



Autonome Technologiesysteme

Eine europäische Perspektive

Autonome Technologiesysteme gelten allgemein als emergente, disruptive Technologien (EDT). Sie gewinnen zunehmend an Bedeutung und haben erheblichen Einfluss auf zukünftige Fähigkeiten in zahlreichen Domänen. Der Aktionsplan der Europäischen Kommission für Synergien zwischen ziviler Industrie, Weltrauminfrastruktur und Verteidigungsindustrie stuft sie als kritische Technologien ein. Sowohl in der EU als auch in der NATO werden autonome Technologiesysteme als strategische „Enabler" betrachtet.

Gerlof de Wilde

Das Feld der autonomen Technologiesysteme entwickelt sich rasant weiter. Im Verteidigungsbereich finanziert die Europäische Union durch den Europäischen Verteidigungsfonds (European Defence Fund, EDF) zahlreiche Projekte im Bereich Forschung, Entwicklung und Investment. Bereits zuvor geschah dies über Vorläuferprogramme wie der Preparatory Action on Defence Research (PADR) sowie durch das Entwicklungsprogramm für die

europäische Verteidigungsindustrie (European Defence Industrial Development Programme, EDIDP).

Ähnliche Projekte werden im intergouvernementalen Rahmen der Ständigen Strukturierten Zusammenarbeit (Permanent Structured Cooperation, PESCO) durchgeführt. Zudem gibt es innerhalb der Europäischen Verteidigungsagentur (European Defence Agency, EDA) verschiedene Initiativen und Projekte, die autonome Systeme in unbemannte Fahrzeuge für Kampfeinsätze integrieren sollen (CAT-B-Projekte). Darüber hinaus wird ein Aktionsplan für autonome Systeme für den Verteidigungsbereich entwickelt. Die Verteidigungsindustrie fordert außerdem die Erarbeitung eines koordinierten EU-Aktionsplans zur Entwicklung von autonomen Landsystemen.

Marktprognosen zufolge ist mit einem enormen Wachstum im Bereich der autonomen Systeme und der zugrunde liegenden Technologien zu rechen. Im Verteidigungsbereich wird erwartet, dass sich das gesamte Marktvolumen von 41 Milliarden US-Dollar im Jahr 2022 auf bis zu 90 Milliarden US-Dollar im Jahr 2030 mehr als verdoppelt.

Unbemannte Systeme wurden bereits in zahlreichen Szenarien eingesetzt, um die Durchhaltefähigkeit von Missionen zu steigern, die Sicherheit und Verlässlichkeit zu erhöhen und Risiken und Kosten zu reduzieren. Langweilige, schmutzige und gefährliche Aufgaben gehören zu den vorrangigen Einsatzfeldern solcher Systeme. Derartigen Systemen ein gewisses Ausmaß an Autonomie zu gewähren, vergrößert die Bandbreite ihrer Einsatzmöglichkeiten und würde ihren Nutzen maximieren. Dank Künstlicher Intelligenz (KI) sind autonome Systeme in der Lage, Menschen in verschiedenen Bereichen zu übertreffen – wie etwa bei der Verarbeitung großer Datenmengen, der Lösung komplexer Probleme und der raschen Entscheidungsfindung. Im Allgemeinen wird Autonomie benötigt oder besonders gewürdigt, wenn

- die Kadenz der Entscheidungsfindung die Beschränkungen durch Kommunikationskanäle übertrifft (z.B. durch Verzögerungen, limitierte Bandbreite oder Kommunikationsfenster),
- zeitkritische Entscheidungen durch das System bzw. an Bord des Fahrzeugs getroffen werden müssen (z.B. Kontrolle, Gesundheit, lebenserhaltende Maßnahmen etc.),
- Entscheidungen durch die Nutzung von großen Mengen an Borddaten verbessert

werden können – im Vergleich zu übermittelten Daten (z.B. adaptive science),
- lokale Entscheidungen die Robustheit verbessern sowie die Komplexität der Systemarchitektur verringern und
- autonome Entscheidungen die Kosten eines Systems reduzieren oder dessen Leistung verbessern.

Zusammengefasst können autonome Systeme zur Verbesserung von Aktivitäten in allen Phasen des Observierungs-, Orientierungs-, Entscheidungs- und Handlungszyklus beitragen.

Als autonome Systeme bzw. autonome Systemtechnologien können Systeme definiert werden, die spezifische Aufgaben in einem definierten Kontext innerhalb eines festgelegten Zeitrahmens erfüllen können. Dies ermöglicht es Personen in vorab definierten Rollen, auf spezifische Weise einzugreifen oder Kontrollfunktionen wahrzunehmen. Gleichzeitig kann das System unter vorherbestimmten Umständen eigenständig Wahrnehmung, Planung und Handlung übernehmen. Autonome Systemtechnologien sind darüber hinaus Technologien, die als „Enabler" für autonome Systeme dienen.

Ein autonomes System erfordert also ein gewisses Maß an „Intelligenz". Es benötigt ein Modell der Welt, muss eine Wahrnehmungskapazität haben und innerhalb des Rahmens einer ausdefinierten Aufgabe arbeiten können, beispielsweise in Form einer Hilfs- oder Zielfunktion. Autonome Systeme können als eigenständige, einzelne Einheiten oder in Form eines „Schwarms" (mehrere Einheiten) funktionieren. Ein autonomes robotisches System (ARS) stellt ein autonomes System dar, das auf eine spezifische Hardware-Plattform angewendet wird, wie beispielsweise ein unbemanntes Boden-, Luft- oder Seefahrzeug. Ein ARS steht vor der zusätzlichen Herausforderung, in der Welt, in der es operiert, zu navigieren.

Bereiche für die Verbesserung von Fähigkeiten in der europäischen Verteidigung werden durch die EDA Common Defence Policy (CDP) priorisiert. Diese inkludieren Fähigkeiten zum Kampf am Boden, verbesserte Logistik und medizinische Unterstützungsfähigkeiten, maritime Manövrierfähigkeit, Unterwasser-Kontrolle – was zur Resilienz auf dem Meer beiträgt – und Luftüberlegenheit und -mobilität. Die CDP trägt auch zur Stärkung reaktiver Cyber-Verteidigungsoperationen bei, ermöglicht die Entwicklung weltraumbasier-

ter Fähigkeiten wie Informations- und Kommunikationsservices, integriert militärische Luftfähigkeiten in einem sich wandelten Luftfahrtsektor und implementiert domänenübergreifende Fähigkeiten, die zum Ambitionsniveau der EU beitragen.

Konkreter soll die EDA CDP die folgenden Aspekte unterstützen: Überwachung, Detektion und Identifikation, Kampfunterstützung, Maßnahmen gegen Minen bzw. Drohnen, Such- und Rettungsdienste, das Monitoring von chemischen, biologischen, radiologischen und nuklearen (CBRN) Wirkstoffen sowie die Dekontamination, die Entsorgung von explosiver Artilleriemunition, die Logistik (Konvois) und die (medizinische) Versorgung und Zieltäuschung bzw. -anlockung.

Zudem können autonome Systeme Kampffähigkeiten unterstützen, indem diese direkt oder indirekt Feuerunterstützung leisten, die Force Protection erhöhen sowie die Fähigkeiten im Bereich Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) unterstützen.

Der Einsatz autonomer Systeme im Militärbereich gestaltet sich herausfordernd. Gründe dafür sind unstrukturierte und schwierige Umgebungen, legale und ethische Probleme im Zusammenhang mit dem Einsatz von Gewalt, ein Mangel an verteidigungsspezifischen Daten für Machine Learning (ML) und mögliche Störungsaktionen durch Gegner. Bedeutungsvolle menschliche Kontrolle ist ein rechtlich und ethisch relevantes Element bei der Nutzung autonomer Systeme in allen Bereichen. Das gilt insbesondere für den Verteidigungsbereich, wenn die Gefechtsführung und die Anwendung von Gewalt Teil der Aufgaben des Systems sind. In solchen Fällen erfährt Autonomie besonderer Aufmerksamkeit.

Bedeutungsvolle menschliche Kontrolle umfasst mindestens die nachstehenden drei Elemente:

1. Menschen treffen informierte, bewusste Entscheidungen über den Einsatz von Waffen.
2. Menschen sind ausreichend informiert, um sicherzustellen, dass – unter Berücksichtigung der verfügbaren Informationen über das Ziel, die Waffe und den Kontext, in dem sie eingesetzt wird – die Anwendung von Gewalt den Regeln des internationalen Rechts entspricht.
3. Die betreffende Waffe wurde für ein realistisches Operationsszenario entworfen und in einem solchen getestet. Die

involvierten Personen haben eine angemessene Ausbildung erhalten, um sicherzustellen, dass sie die Waffe verantwortungsbewusst einsetzen.

Zusammenfassend lässt sich sagen, dass autonome Systemtechnologien künftige Verteidigungsfähigkeiten maßgeblich beeinflussen werden, und das disruptiv. KI-Technologien werden die Entscheidungsfindung in autonomen Systemen ermöglichen. Für den Verteidigungsbereich bedeutet dies, dass bedeutungsvolle menschliche Kontrolle und die Vorgaben des internationalen Rechts die zukünftige Entwicklung leiten werden.

Gerlof de Wilde ist in der Generaldirektion Verteidigungsindustrie und Weltraum (DG DEFIS) der Europäischen Kommission tätig.

Shutterstock

Die KI-Strategie des BMLV

Die KI-Strategie des Bundesministeriums für Landesverteidigung (BMLV) zielt darauf ab, Künstliche Intelligenz (KI) systematisch in die militärischen und administrativen Prozesse zu integrieren. Diese Integration soll dazu dienen, die Effizienz und Effektivität der Abläufe zu steigern und die Wettbewerbsfähigkeit sowie Innovationskraft des Österreichischen Bundesheeres (ÖBH) nachhaltig zu sichern. Im Kontext der fortschreitenden digitalen Transformation wird KI als entscheidende Technologie betrachtet, um die Herausforderungen einer zunehmend komplexen sicherheitspolitischen Lage zu bewältigen und Effekte, Effizienzsteigerung und Ausgleich der demografischen Entwicklung sicherzustellen.

Arnulf Kopeinig

Strategische Absicht

Die digitale Transformation erfordert eine strategische Neuausrichtung des BMLV im Umgang mit KI. Diese Technologie wird als zentraler Hebel angesehen, um komplexe, datenintensive Aufgaben effektiver zu bewältigen und sowohl militärische als auch nicht-militärische Prozesse zu optimieren. Die stetig wachsende Menge an Daten und die Notwendigkeit, schnelle und fundierte Entscheidungen zu treffen, machen den Einsatz von KI unverzichtbar. Die umfassende

Digitalisierung der Streitkräfte und der Verwaltungsprozesse ist eine zentrale Voraussetzung, um die Effektivität und Effizienz der Aufgabenwahrnehmung zu erhöhen.

Die Strategie des BMLV verfolgt das Ziel, durch den gezielten Einsatz von KI die Herausforderungen der technologischen Veränderungen und der digitalen Transformation zu meistern. Eine strukturierte und technologieagnostische Herangehensweise soll sicherstellen, dass die dynamischen Entwicklungen von KI kontinuierlich beobachtet und adäquat in die Prozesse des BMLV integriert werden. Dies erfordert eine enge Verzahnung von Technologieentwicklung und organisatorischen Anpassungen. Hierfür soll eine zentrale Stelle innerhalb des Ressorts aufgestellt werden, die diese Strategie umsetzen soll.

Leitlinien und Handlungsfelder

Die Strategie definiert wie folgt mehrere Handlungsfelder, um die Integration von KI zu steuern.

Governance und Organisation: Eine zentrale Steuerung und klare Zuständigkeiten sollen sicherstellen, dass KI-Anwendungen ordnungsgemäß geplant, entwickelt, getestet und betrieben werden. Es wird eine zentrale verantwortliche Stelle eingerichtet, die alle KI-bezogenen Maßnahmen koordiniert und überwacht. Durch Governance werden die Prinzipien festgelegt, nach denen KI-Anwendungen entwickelt und betrieben werden. Dies umfasst auch die Sicherstellung der Überprüfbarkeit von KI-Systemen und ihrer Verwendung über den gesamten Lebenszyklus hinweg.

Leistungsbereiche: Der Einsatz von KI soll dazu beitragen, die Arbeitsbelastung zu verringern und Ergebnisse zu optimieren. Dies betrifft insbesondere komplexe Prozesse, wie Führungsunterstützung (C2), strategische Planung, Logistik, Militärmedizin und Cyber-Operationen. KI soll außerdem helfen, demografische Herausforderungen abzufedern. Durch die Integration von marktorientierten Anwendungen kann der Nutzen von zivilen Technologien auch für militärische Zwecke ausgeschöpft werden.

Agilität: Organisatorische Flexibilität und Anpassungsfähigkeit sind entscheidend, um mit den schnellen Technologiezyklen Schritt zu halten. Die Strukturen und Prozesse müssen so gestaltet werden, dass sie rasch auf technologische Veränderungen reagieren können und auf die Entwicklungen im Reifegrad von KI angepasst sind. Dies erfordert eine proaktive und

initiativreiche Herangehensweise, um notwendige Veränderungen zeitnah umzusetzen.

Personal: Der nachhaltige Aufbau und Erhalt von Fachwissen im Bereich KI ist notwendig. Dies umfasst die Rekrutierung und Ausbildung von Expertinnen und Experten sowie die Förderung der Diversifizierung des Fachpersonals. Es ist unumgänglich, das BMLV als attraktiven Arbeitgeber zu positionieren, um qualifiziertes technisches Fachpersonal anzuziehen und zu halten. Flexible Arbeitsmodelle sollen gefördert werden, um die Motivation und Leistungsfähigkeit der Mitarbeiterinnen und Mitarbeiter zu steigern.

Ausbildung und Literacy: Ressortangehörige sollen ein grundlegendes Verständnis für KI entwickeln, um deren Einsatz optimal zu gestalten. Dies umfasst die Einführung umfassender Schulungsprogramme zur Vermittlung wesentlicher Prinzipien und Anwendungen von KI, sowie die kontinuierliche Anpassung von Kompetenzen aller Mitarbeiterinnen und Mitarbeiter. Moderne Lernplattformen und Simulationstools sollen genutzt werden, um praxisnahe und interaktive Lernumgebungen zu schaffen. Ein besonderer Fokus liegt dabei auf der KI-Literacy, also der Fähigkeit, die Funktionsweisen und Einsatzmöglichkeiten von KI zu verstehen und kritisch zu hinterfragen.

Neue Arbeitsplatztypen: Die Integration von KI und neuen Technologien wird zur Entstehung neuer Arbeitsplatztypen führen. Diese neuen Rollen werden spezialisierte Fähigkeiten und Kenntnisse erfordern, die über das traditionelle Ausbildungsprofil hinausgehen.

Vertrauen: Das Vertrauen in KI-Systeme wird durch die Kombination von Cyber-Sicherheit und ethischen Standards gefördert. Es ist wichtig, dass die Systeme zuverlässig, vorhersehbar und sicher sind. Durch aktive Kommunikation und Transparenz in der Entwicklung und Anwendung von KI soll das Vertrauen in diese Technologien gestärkt werden.

Normen und Standards: Der Einsatz von KI erfolgt auf Grundlage nationaler und internationaler Rechtsvorschriften, die sich an die jüngsten bzw. kommende Entwicklungen in Hinblick auf KI-Anwendungen in Zukunft angepasst werden können. Ethische Standards sind ebenfalls von zentraler Bedeutung, insbesondere in Bezug auf die menschliche Kontrolle und den vertrauenswürdigen Einsatz von KI. Der Akkreditierungsprozess komplexer KI-Systeme soll dahingehend angepasst werden.

Verteidigungspolitische Positionierung: Das BMLV verpflichtet sich zur verantwortungsvollen Nutzung von KI im Rahmen der relevanten Normen und Standards sowie zur Gewährleistung des Schutzes der Soldatinnen und Soldaten. KI soll dazu beitragen, die Fähigkeiten des ÖBH zu verbessern und die militärische Landesverteidigung zu stärken. Eine bedeutungsvolle menschliche Kontrolle bleibt dabei unerlässlich.

Grundlagen der KI-Integration

Verfügbare KI-Modelle werden nur nach gesamtheitlicher Beurteilung, insbesondere hinsichtlich des entstehenden Risikos, sowie nach Durchlaufen strenger Verifizierung, Validierung und Zertifizierung und ausreichender Auditierung durch das BMLV integriert.

Die Marktorientierung ist ein wesentlicher Aspekt der KI-Strategie des BMLV. Projekte und marktfähige Lösungen der KI können grundsätzlich alle Leistungsbereiche des BMLV betreffen. In der Regel ist es jedoch nicht möglich, eine marktfähige KI-Anwendung zu kaufen, zu installieren und unmittelbar für Zwecke des BMLV zu nutzen. Daher kommt neben Integration und Anpassung dem Projekt- und Innovationsmanagement besondere Bedeutung zu. Anwendungen der KI sind überwiegend „Dual-Use"-Anwendungen. Ihre Verwendung wird sowohl im sicherheitsbezogenen Umfeld als auch für zivile Zwecke erfolgen. Kurzfristig sind insbesondere vielfältige „Dual-Use"-fähige Kleinanwendungen zu erwarten.

Für die Integration von KI bedarf es nicht nur Maßnahmen für die eigene Informations- und Kommunikationstechnologie-Infrastrukturumgebung, sondern auch einer Anpassung der beteiligten Prozesse und Regularien sowie gegebenenfalls personeller und ausbildungsorientierter Begleitmaßnahmen. Interne Richtlinien von Beschaffungsabläufen sind hinsichtlich einer Beschleunigung von KI-Vorhaben zu evaluieren und gegebenenfalls anzupassen.

Das Ökosystem „Verteidigung-Wirtschaft-Forschung" bildet die Basis für eine erfolgreiche Umsetzung der KI-Strategie des BMLV. Die Zusammenarbeit zwischen diesen Bereichen ist entscheidend, um innovative Lösungen zu entwickeln und die Wettbewerbsfähigkeit zu sichern. Für Kooperationen mit Instituten aus dem wissenschaftlich-forschenden, universitären Bereich, dem Bereich der Forschungsunternehmen, dem industriell entwickelnden und fertigenden Bereich sowie

aus den Start-Ups werden bevorzugt nationale Partner ausgewählt. Forschungsvorhaben dieser Stellen werden durch Fachexpertise des Ressorts fachlich lenkend unterstützt. Dadurch wird interne Expertise aufgebaut und ein Netzwerk innerhalb des KI-Ökosystems gebildet, das für eigene Vorhaben ein zeitsparendes Vorgehen ermöglicht.

Die Prozesse für Forschung, Entwicklung und Bereitstellung im BMLV sind kontinuierlich zu optimieren. Darüber hinaus ist die aktive Teilnahme an relevanten Forschungsprojekten auf EU-Ebene und mit internationalen Partnern weiterhin erforderlich. Damit können Synergieeffekte zwischen nationaler und internationaler Bearbeitung und Forschung zu militärischen KI-Anwendungen erreicht werden. Dies betrifft sowohl die Entwicklung von Rüstungssystemen als auch die Förderung von „Dual-Use"-Produkten. Aus zeitlichen und aus Ressourcengründen ist die eigenständige Forschung des BMLV zur Entwicklung von Anwendungen im Bereich der Technologiegruppe KI nachrangig.

Die Integration von KI-Produkten, sei es vom Markt oder aus Forschungskooperationen, ist in jedem Projekt möglichst rasch und agil umzusetzen. Hierfür sollen Anbieter von Lösungen flexibel herangezogen werden. Auch strategische Partnerschaften, sowohl mit österreichischen als auch global agierenden IT-Firmen, sind für diese Zwecke nicht auszuschließen.

Zentrale Umsetzungsschritte

Technologie-Monitoring und Evaluierung: Es ist notwendig, die technologischen Entwicklungen im Bereich KI kontinuierlich zu beobachten und zu bewerten, um deren Potenzial für militärische und administrative Anwendungen zu identifizieren. Durch systematisches Monitoring können frühzeitig Trends erkannt und entsprechende Maßnahmen ergriffen werden.

Neugestaltung von Prozessen: Bestehende Prozesse müssen unter Berücksichtigung der technologischen Möglichkeiten von KI neugestaltet werden. Dies erfordert eine enge Zusammenarbeit zwischen den verschiedenen Bereichen des BMLV. Die Prozessanpassung durch KI-Unterstützung wird angestrebt, um die Effizienz zu steigern und die Qualität der Ergebnisse zu verbessern.

Zentrale Steuerung und dezentrale Umsetzung: Es ist erforderlich, eine Balance zwischen zentraler Steuerung und dezentraler Ent-

wicklung zu finden, um die effiziente Implementierung von KI zu gewährleisten. Klare Zuständigkeiten und Entscheidungsbefugnisse sind dabei entscheidend. Die dezentrale Umsetzung ermöglicht eine flexible Anpassung an spezifische Anforderungen und Gegebenheiten.

Qualifizierung des Personals: Das Personal muss kontinuierlich weitergebildet und auf die Nutzung von KI vorbereitet werden. Dabei ist wichtig, dass die Mitarbeiterinnen und Mitarbeiter die notwendigen Kompetenzen erwerben und weiterentwickeln, um die neuen Technologien effektiv einsetzen zu können. Fortbildungsprogramme und Schulungen sollen regelmäßig angeboten werden, um den Wissensstand stets aktuell zu halten.

Rechtliche Rahmenbedingungen und ethischer Einsatz: Sowohl rechtliche Rahmenbedingungen als auch ethische Standards werden in allen Phasen der Entwicklung und Nutzung von KI berücksichtigt. Dies umfasst die Entwicklung, Beschaffung, Einführung und Nutzung der Systeme. Ethische Beurteilungen fließen in das Risikomanagement ein und tragen dazu bei, dass KI-Systeme sicher und verantwortungsvoll eingesetzt werden.

Kooperationen und Netzwerke: Nationale und internationale Kooperationen sollen den Wissenstransfer fördern und Synergieeffekte nutzen. Durch Kooperationen mit Wissenschaft und Industrie sollen innovative Lösungen entwickelt und implementiert werden. Das BMLV wird sich aktiv an Netzwerken und Gremien beteiligen, um den Austausch von Wissen und Erfahrungen zu fördern.

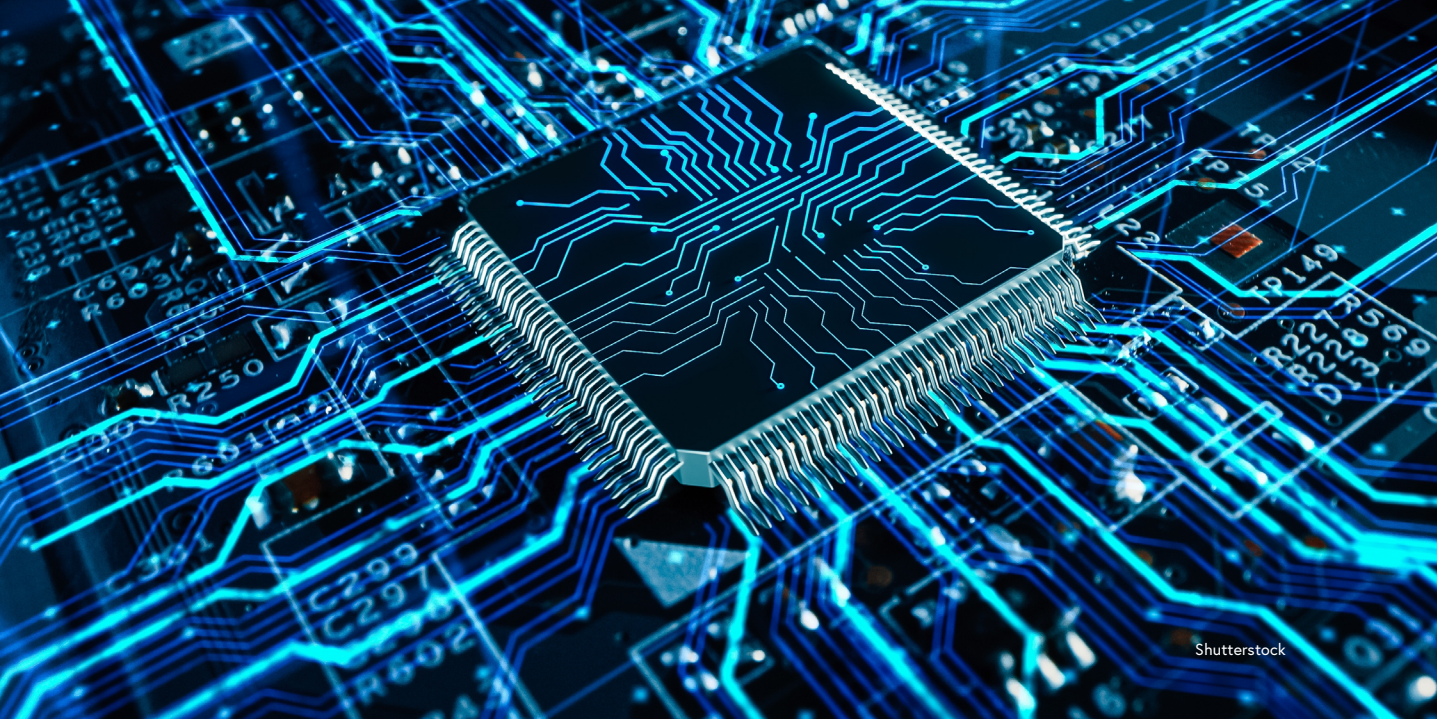
Fazit

Die KI-Strategie des BMLV bietet eine flexible, umfassende und strukturierte Herangehensweise zur Nutzung von KI für militärische und nicht-militärische Anwendungen. Durch die systematische Integration von KI sollen Effizienz und Wettbewerbsfähigkeit gesteigert werden. Die Strategie erfordert eine kontinuierliche Anpassung und Weiterentwicklung. Nur durch eine enge Verzahnung von Technologieentwicklung, organisatorischen Anpassungen und qualifizierten Mitarbeitern kann das BMLV das volle Potenzial von KI ausschöpfen.

Organisatorische und menschenorientierte Aspekte spielen dabei eine zentrale Rolle, um eine erfolgreiche Implementierung und nachhaltige Nutzung von KI zu gewährleisten. Die Zusammenarbeit mit

Brigadier Arnulf Kopeinig ist Leiter der Abteilung Informations- und Kommunikationstechnologie-Planung im BMLV und zeichnet federführend für die KI-Ressortstrategie des BMLV verantwortlich.

Wirtschaft und Forschung ist essenziell, um innovative Lösungen für zukünftige Herausforderungen zu entwickeln. Die Ausbildung und kontinuierliche Weiterbildung des Personals sowie die Schaffung neuer Arbeitsplatztypen sind entscheidende Elemente, um die Potenziale der KI voll auszuschöpfen und die Transformation erfolgreich zu gestalten.


Shutterstock

Künstliche Intelligenz in der Cyber-Verteidigung

Bereits vor der medialen Wahrnehmung von ChatGPT eröffnete Künstliche Intelligenz (KI) faszinierende Möglichkeiten für viele Anwendungsgebiete. Dazu gehört erwartungsgemäß auch die Verteidigungsindustrie, insbesondere im Bereich der Cyber-Sicherheit und-Verteidigung, wo maschinelles Lernen und KI in verschiedenen Kontexten eingesetzt werden. Dies bringt zahlreiche Chancen, jedoch auch Herausforderungen und Risiken mit sich.

Victoria Toriser
Florian Silnusek

Chancen und Anwendungsfelder

Im Bundesministerium für Landesverteidigung (BMLV) wird KI vielseitig verwendet, insbesondere um den Faktor Mensch zu unterstützen. Seit 2023 sind etwa in speziellen Bereichen der Cyber-Sicherheit bereits KI-Systeme im produktiven Einsatz. Im Österreichischen Bundesheer (ÖBH) tragen Pilotinstallation zum Erfahrungs- und Erkenntnisgewinn bei. KI unterstützt die Vorfalls- und Malware-Analyse dabei, Anomalien im Verhalten von Netzwerken und Geräten zu erkennen, die auf Angriffe hinweisen. Im BMLV werden zudem adaptierte Deep-Learning-

Modelle zur Klassifizierung von Dateien mit dem Fokus auf eingebettete Malware oder sonstige Angriffsvektoren verwendet.

Im Bereich Forschung und Entwicklung zielt das auf EU-Ebene geplante Projekt „Artificial Intelligence Deployable Agent" darauf ab, einen gemeinsamen europäischen Rahmen zu entwickeln, der Anwenderinnen und Anwender sowie Entscheidungsträgerinnen und -träger in verschiedenen Szenarien unterstützen soll. Dieses Projekt mit österreichischer Beteiligung, das 2024 gestartet wurde, integriert KI-basierte Cyber-Verteidigungsagenten, die autonome und halbautonome Aktionen durchführen und den gesamten Lebenszyklus eines Cyber-Vorfalls abdecken. Das Projekt befasst sich mit zwei wesentlichen Herausforderungen, mit denen Endnutzerinnen und -nutzer im Verteidigungssektor konfrontiert sind: einerseits eine wachsende Angriffsfläche aufgrund der zunehmenden Digitalisierung und andererseits die Verwendung von KI-basierten Lösungen durch Angreiferinnen und Angreifer.

KI wird bereits vielfach und vielseitig im Cyber-Sicherheitsbereich eingesetzt, und ihre Bedeutung wird weiter steigen. Dabei bringt sie zahlreiche Vorteile mit:

- In der Vorfalls- und Malware-Analyse trägt KI dazu bei, Anomalien im Verhalten von Netzwerken und Geräten zu erkennen, die auf einen Angriff hinweisen. Adaptierte Deep-Learning-Modelle können beispielsweise zur Klassifizierung von Dateien mit dem Fokus auf eingebettete Malware oder sonstige Angriffsvektoren eingesetzt werden.
- KI verbessert die Bedrohungserkennung und -reaktion, indem sie rasch große Datenmengen analysiert. Dies ermöglicht es, zeitnah auf Bedrohungen zu reagieren, Cyber-Angriffe schneller zu erkennen und dadurch Schäden zu minimieren.
- KI unterstützt bei der Bewältigung der Datenflut und trägt so zu einem verbesserten Situationsbewusstsein und zur Entscheidungsfindung bei. Sicherheitspersonal wird rasch mit verwertbaren Erkenntnissen versorgt, die bessere Entscheidungen ermöglichen.

Eine besondere Rolle spielt KI zudem im Rahmen der Cyber-Range-Technologien. Eine Cyber Range ist eine spezialisierte Trainings- und Simulationsumgebung, die entwickelt wurde, um Cyber-Sicherheitsfähigkeiten zu schulen und zu testen. Sie bietet eine sichere, kontrollierte Umgebung, in der

Teilnehmerinnen und Teilnehmer reale Cyber-Angriffe und Verteidigungsszenarien nachstellen und üben können. Dies hilft Sicherheitsteams, ihre Fähigkeiten zu verbessern, ohne Risiken für tatsächliche Systeme einzugehen.

KI kann in Cyber Ranges eingesetzt werden, um realistische und dynamische Bedrohungssimulationen zu erstellen, personalisierte Trainingsprogramme zu entwickeln, Echtzeit-Analysen und Feedback zu bieten sowie Verhaltensmuster zu erkennen und zu analysieren. Sie ermöglicht automatisierte Bewertungen und Berichtserstellung, integriert aktuelle Bedrohungsinformationen und bietet Unterstützung durch virtual assistants bzw. Mentorinnen und Mentoren. Diese Anwendungen verbessern Effektivität und Effizienz der Trainingsumgebungen und bereiten die Teilnehmerinnen und Teilnehmer besser auf reale Bedrohungen vor.

Herausforderungen

Neben zahlreichen Erfolgsgeschichten scheint die KI im öffentlichen Bewusstsein einen wichtigen Stellenwert erreicht zu haben. Allerdings erfüllt KI hochgesteckte Erwartungen in manchen Fällen noch nicht; manchmal werden Limitationen des Systems aufgezeigt. KI-Systeme haben beispielsweise den Ruf, fehleranfällig zu sein, da die Systeme noch nicht robust und verlässlich genug sind, um in jeder Situation zu funktionieren. Im Bereich der Cyber-Verteidigung heißt das, dass fälschlicherweise Anomalien oder Hinweise auf Angriffe indiziert werden („False Positives"). Des Weiteren ruft mangelnde Transparenz und Interpretierbarkeit vieler KI-Systeme bei Expertinnen und Experten Bedenken hervor. KI-Systeme sind oft undurchsichtige „Black Boxes", was es schwierig macht zu verstehen, wie sie Entscheidungen treffen und daraus lernen.

Weiters äußern Sicherheitsexpertinnen und -experten Bedenken hinsichtlich systematischer Fehler oder Verzerrungen in KI-Modellen (Bias). Hierbei sind die Qualität der Trainingsdaten und die verwendeten Algorithmen entscheidend. Ist die Qualität der Trainingsdaten mangelhaft, kann sich dies in einem Bias niederschlagen, was sich wiederum negativ auf die Leistung eines KI-Systems auswirken kann.

KI-Lösungen sind am effektivsten, wenn sie gut in die vorhandene Sicherheitsarchitektur integriert sind. Die mangelhafte oder unvollständige Integration in die bestehende Sicherheitsinfrastruktur oder die Inkompatibilität mit ande-

Dipl.-Ing. Florian Silnusek ist Leiter der Abteilung Cybersicherheit Technik des Militärischen Cyberzentrums.

Mag. Victoria Toriser ist die Leiterin des Referats Cyber Grundlagen und Innovation des Militärischen Cyberzentrums.

ren Systemen schränkt den Nutzen des KI-Systems ein.

Aufgrund dieser Herausforderungen befasst sich das BMLV im Bereich der Cyber-Sicherheit im Rahmen eines nationalen Projekts intensiv mit den Risiken und Gefahren, die sich aus dem Einsatz von KI durch externe (d.h. andere staatliche und nichtstaatliche) Akteure für die einsatzrelevanten Informations- und Kommunikationstechnologiesysteme des ÖBH ergeben. Die Ergebnisse des Forschungsprojekts sollen die Handlungsfähigkeit des ÖBH auf dem Gebiet der KI stärken, indem sie ein möglichst umfassendes Bild der aktuellen Risiko- und Bedrohungslage zeichnen. Die Ergebnisse richten sich dahingehend sowohl an technisch versierte Spezialistinnen und Spezialisten als auch an Entscheidungsträgerinnen und -träger, die auf Basis der gewonnenen Erkenntnisse die aktuelle Situation besser einschätzen sowie weitere notwendige Schritte im Umgang mit KI planen und umsetzen können.

Konsequenzanalyse und notwendige Maßnahmen

KI-Sicherheit muss über die Grenzen der Software- und Hardware-Implementierung hinausgehen und innerhalb der Triade von Technologie, Anwendungsfall und Mensch im Kreislauf verstanden werden. Ein sicherer und verantwortungsvoller Betrieb von KI ist ein Schlüsselfaktor für den erfolgreichen Einsatz in verschiedenen Domänen. Ziel dessen ist primär die Absicherung gegen Risiken und Bedrohungsszenarien. Ein wesentlicher Teil der Diskussion konzentriert sich auf zwei Konzepte im Zusammenhang mit der Einbeziehung menschlicher Interaktion in automatisierte Prozesse und Systeme. Beim Ansatz „Human in the Loop“, der die direkte menschliche Interaktion und Kontrolle über KI-Systeme beinhaltet, wird sichergestellt, dass menschliches Urteilsvermögen integraler Bestandteil des Entscheidungsprozesses bleibt. Beim Ansatz „Human on the Loop“ überwachen Menschen die KI-Operationen und greifen bei Bedarf ein, wobei sie eine überwachende Rolle anstelle direkter Kontrolle übernehmen.

Trotz Fortschritten in der KI ist es relevant, dass die letztendliche Entscheidungsgewalt bei menschlichen Entscheidungsträgerinnen bzw. -trägern verbleibt. KI dient als Unterstützungssystem, das wertvolle Daten und Analysen zur Information bereitstellt, soll jedoch keine autonomen Entscheidungen treffen.

Bundesministerium
Landesverteidigung