Lebenslanges Lernen

Digitalisierung und KI stellen die Bundeswehr vor neue Herausforderungen

Klaus Hardy Mühleck | **Bei der Beschäftigung mit KI haben das Verteidigungsministerium und die Bundeswehr bereits einiges geleistet. Doch bei manchen neuen Fragen, beispielsweise wie sich KI auf militärische Führungsfähigkeiten auswirken wird, gibt es noch Klärungsbedarf. Solche Fragen müssen ressortübergreifend und mit Partnern angegangen werden.**

Die Bundeswehr beschäftigt sich seit einiger Zeit im Kontext ihrer Digitalisierung mit KI-Einsatzmöglichkeiten sowie den aktuellen und zukünftigen Herausforderungen im Cyberraum. Um diesen gerecht werden zu können, wurden 2016 eine ministerielle Abteilung Cyber und Informationstechnik (CIT) und 2017 ein neuer Organisationsbereich Cyber- und Informationsraum (CIR) aufgebaut mit dem Ziel, die Dimension Cyber- und Informationsraum unter einheitlicher Führung zu steuern. Mit dem Leiter der Abteilung CIT im Bundesministerium der Verteidigung (BMVg) hat die Bundeswehr auch erstmalig einen Ressort Chief Information Officer (CIO).

KI-Technologien verbreiten sich schon jetzt rasant – man denke nur an Siri und Alexa, die einem im Alltag begegnen – und haben Multi-Use-Charakter. Das erhöht das Risiko des Missbrauchs für kriminelle, politische oder militärische Zwecke. Mehr noch: Digitalisierung und KI haben das Potenzial, Strukturen und Prozesse jeder Organisation zu verändern – auch die der Bundeswehr. Daher bedarf es einer Leitungs-, Steuerungs- und Gestaltungsstruktur, die der Neuartigkeit und „Querschnittlichkeit“ des Themas gerecht wird. Im Geschäftsbereich des BMVg wird der Themenbereich KI gegenwärtig als Teil des Gesamtthemas Digitalisierung behandelt und damit über das Leitungsboard Digitalisierung auf der Leitungsebene des Ministeriums strategisch gesteuert.

Die Bundeswehr ist damit nicht allein. Überall auf der Welt haben Staaten und ihre Streitkräfte die Chancen und Risiken von Digitalisierung und KI identifiziert. Es stellen sich zahlreiche neue, noch zu klärende Fragen, u.a. wie die Auswirkungen der Digitalisierung und die Anwendung von KI die Bereiche Führungsorganisation und Führungsverfahren in den Streitkräften betreffen. Konkret muss man beispielsweise fragen, welche neuen Abhängigkeiten oder auch Vulnerabilitäten im Bereich der Informationstechnologie entstehen

und wie angesichts einer weiter fortschreitenden Automatisierung – zukünftig gegebenenfalls auch in Waffensystemen – die menschliche Kontrolle gewahrt werden kann. Auch werden sich KI-Konzepte und -Technologien nur in Kooperation entwickeln und anwenden lassen. Dabei ist für die Bundeswehr sowohl die europäische als auch die transatlantische Zusammenarbeit wichtig.

Erste Priorität: Informationsversorgung

Die Anwendungsmöglichkeiten für KI in den Streitkräften sind vielfältig und erstrecken sich über das gesamte Fähigkeitsprofil. Das Sicherstellen der Informationsversorgung unter allen Bedingungen sowohl in Deutschland als auch für die Soldatinnen und Soldaten im Einsatz ist Grundlage für eine handlungs- und leistungsfähige Bundeswehr. Die Resilienz des IT-Systems der Bundeswehr und die Eventualfallplanung bei Störung oder Ausfall gewinnen dabei ständig an Bedeutung.

Ein kontinuierlich verfügbares, gesichertes, umfassendes und aktuelles Lagebild ist auch weiterhin die unerlässliche Basis für das eigene militärische Handeln und Entscheiden. Für das eigene Handlungs- und Leistungsvermögen, also das Fähigkeitsprofil der Streitkräfte, kann die Implementierung von KI vorhandene Fähigkeiten verbessern, aber auch in der weiteren Perspektive die Entwicklung neuer Fähigkeiten ermöglichen beziehungsweise erforderlich machen. Dieses umfasst beispielsweise die Verwendung extrem leistungsfähiger Lernalgorithmen im Rahmen einer verbesserten Krisenfrüherkennung, die Analyse sehr großer Datenmengen (Big Data) oder auch den Einsatz von KI im Bereich des Personalmanagements, bei der Logistik, dem Energiemanagement oder bei Vorhersagen.

KI kann Entscheidungen effizient und effektiv unterstützen

Das enorme Potenzial von KI liegt darin, Entscheidungen effizient und effektiv zu unterstützen und ist aus militärischer Perspektive eine der bedeutendsten Facetten der Digitalisierung. Grundsätzlich lässt die Digitalisierung mit Blick auf KI im militärischen Kontext u.a. eine extreme Beschleunigung des Durchlaufens der Entscheidungszyklen sowie die damit einhergehenden Vorteile eines besseren Lagebilds erwarten. Unstrittig ist ebenso, dass KI das Potenzial hat, menschliche Fehlinterpretationen zu verringern. Zudem ist KI absehbar ein „Enabler“ für eine Vielzahl künftiger Anwendungen und ein Motor für die weitere Automatisierung technischer Systeme. Für die Bundeswehr ist es allerdings wichtig, dass von Beginn an bei der Integration immer auch die Nachvollziehbarkeit der auf KI basierten Entscheidungen mit berücksichtigt wird.

Deutschland muss die mit Digitalisierung und KI verbundenen Herausforderungen ressortübergreifend und gemeinsam mit seinen internationalen Partnern und Verbündeten angehen, um beim bereits begonnenen Wettlauf in den wirtschaftlichen und militärischen Anwendungsbereichen nicht den Anschluss zu verlieren. Ein Miteinander im europäischen Kontext und darüber hinaus ist daher – gerade im Bereich der KI – unabdingbar.

Bereits jetzt werden in der Zuständigkeit des Bundesamts für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) Forschungs-

Bild nur in Printausgabe verfügbar

vorhaben durchgeführt, um das Potenzial der KI für Zwecke der Bundeswehr zu überprüfen. Darüber hinaus werden konkrete mögliche Anwendungsfelder wie Cybersicherheit und Bildauswertung untersucht.

Im Rahmen von Studien und Projekten wendet die Bundeswehr bereits vereinzelt KI-Techniken an beziehungsweise testet Anwendungen in ersten Pilotprogrammen. Eines dieser Projekte ist das Gemeinsame Lagezentrum für den Cyber- und Informationsraum (GLZ CIR) des Kommandos Cyber- und Informationsraum. Hier werden alle verbindenden und relevanten Aspekte des Cyber- und Informationsumfelds zu einer militärischen Lage zusammengefügt. Durch die gezielte Gesamtschau der Brückenelemente beider „Welten“ können Phänomene oder Ereignisse der jeweiligen Umgebungen besser eingeordnet und bewertet werden.

Der Cyber- und Informationsraum ist nicht nur weltumspannend, sondern bedient sich auch nahezu aller Sprachen. Meinungsbildung vollzieht sich auf der Grundlage menschlicher Sprachen; die Kommunikation im „Internet of Things“ – der vernetzten Gegenstände – und die zwischen anderen Cyberkomponenten selbst basiert auf künstlichen Sprachen, durch die sich IT-Systeme miteinander verbinden. Für die Analyse der Informationen im Cyber- und Informationsraum werden daher leistungsfähige maschinelle Übersetzungstools angewendet, die die Datengrundlage ebenso wie die Aufbereitung der Lage sowohl in Englisch als auch in Deutsch gewährleisten.

Eine weitere grundsätzliche Herausforderung im Cyber- und Informationsumfeld ist die Attributierung. Wer in der Cyber- und IT-Umgebung operiert, hat die Möglichkeit, seine Absichten und Verhaltensweisen in einer enormen Datenflut zu verbergen. Wenn eine Aktion einen Effekt im Cyber- und Informationsraum auslöst, dann bleibt dem Beobachter oftmals nur die Feststellung,

was passiert ist. In der Regel sind im Umfeld beabsichtigte oder unbeabsichtigte Effekte erster, zweiter oder weiterer Ordnung zu messen. Schließt man rein vom gemessenen Effekt auf die Ursache und somit auf die Motivationslage des Verursachers, kann es zu Fehleinschätzungen kommen. Diese Herausforderung der Attributierung lässt sich auch im GLZ CIR nicht umfassend lösen. Allerdings werden dort Ereignisse, auch solche erweiterter Ordnung, mit solchen Daten korreliert, die bereits bekannt sind und bestimmten Akteuren zugewiesen werden können. Durch die mathematische Aufbereitung der Daten und eine komplexe Netzwerkanalyse kann so eine strukturierte Aussage über mögliche Zusammenhänge getroffen werden. Dazu werden Entitäten unter Nutzung von KI-Techniken automatisch aus unstrukturierten und strukturierten Daten extrahiert und schließlich ein Beziehungsgeflecht generiert, das durch soziale und technische Graphen abgebildet wird. Mithilfe von KI wird also das GLZ CIR zukünftig ein ganzheitliches Bild von Problembereichen an der Schnittstelle zwischen Cyber/IT und Informationsraum ermitteln, darstellen und bewerten können.

Die Bundeswehr will auch das Know-how von Start-ups nutzen

Vernetztes Vorgehen

Der politische Gestaltungsanspruch im Bereich der KI wird auch im Koalitionsvertrag der Regierungsparteien an zahlreichen Stellen hervorgehoben. Die Plattform „Lernende Systeme – Plattform für Künstliche Intelligenz“ soll in ein nationales Forschungskonsortium für KI und maschinelles Lernen aufwachsen. Gemeinsam mit Frankreich soll ein öffentlich verantwortetes KI-Zentrum errichtet werden. Der nationale „Masterplan KI“ soll alle diese Elemente verbinden.

Um auch das Know-how der Start-up-Szene im Bereich KI zu erschließen, wurde im Jahr 2017 das Cyber Innovation Hub (CIH) gegründet, das als Bindeglied zwischen den Start-ups und der Bundeswehr fungiert. Auch das an der Universität der Bundeswehr München seit 2017 im Aufbau befindliche Cyber-Cluster wird sich zukünftig mit mehreren Professuren u.a. dem Thema KI widmen. Unterstützt von einem strukturierten Dialog zwischen dem BMVg und den Industrieverbänden werden die Erkenntnisse sämtlicher Forschungs- und Innovationsaktivitäten mit dem Forschung & Technologie (F&T)- und Innovationsmanagement Cyber/IT in der Bundeswehr gebündelt und mit dem Bedarfsträger in den Streitkräften, dem Kommando Cyber- und Informationsraum sowie den zukünftigen Nutzern in der Bundeswehr bewertet. Ziel ist es, auf dieser Basis die Fähigkeiten bedarfsgerecht und entlang der politischen Vorgaben auszubauen.

Sicher werden Digitalisierung und Künstliche Intelligenz menschliche Tätigkeiten stark verändern. Das Konzept des „lebenslangen Lernens“ wird darum wichtiger denn je sein – auch für die Bundeswehr.

Klaus Hardy Mühleck ist Leiter der Abteilung Cyber- und Informationstechnik (CIT) im Bundesministerium der Verteidigung und Ressort Chief Information Officer.