Cyberstreiter?

Was Soldatinnen und Soldaten künftig können müssen

Ferdinand Alexander Gehringer
Geboren 1991 in Mannheim, Referent Innere- und Cybersicherheit, Hauptabteilung Analyse und Beratung, Konrad-Adenauer-Stiftung.

Im russischen Angriffskrieg gegen die Ukraine lässt sich noch nicht vollständig erkennen, wie sich die Kriegsführung verändert. Zwar gleicht dieser Krieg mittlerweile einem herkömmlichen Abnutzungskrieg mit schwerem Gerät, dennoch werden vereinzelt Elemente sichtbar, die zeigen, mit welchen Anforderungen die Streitkräfte der Zukunft rechnen müssen.

Die Nutzung von Drohnen in militärischen Konflikten stellt keine Neuerung dar; neu sind die große Anzahl an Drohnen und die Vielzahl der verschiedenen Drohnenmodelle, die in der Ukraine zum Einsatz kommen – von kleinen Drohnen wie die *Black Hornet* bis zur russischen *Orion* mit einer Spannweite von etwa sechzehn Metern, von unbewaffneten DJI-Drohnen[1] für die Aufklärung und bewaffneten Drohnen wie die türkische *Bayraktar TB2* bis hin zu Einwegdrohnen („Kamikazedrohnen"), mit denen Bodentruppen angriffen werden.

1 Dà-Jiāng Innovations Science and Technology Co. (DJI) ist ein Drohnenhersteller aus China.

Absehbar ist, dass künftig verschiedene Drohnentypen – je nach ihren Fähigkeiten – in Drohnenschwärmen miteinander vernetzt in die taktische und operative Kriegsführung auf dem Schlachtfeld integriert werden. So entwickeln die USA zurzeit im Programm *Replicator* kleine, kostengünstige, autonome Drohnensysteme, die durch den Einsatz von Künstlicher Intelligenz (KI) im Schwarm zusammenwirken.[2] Der Einsatz von KI in den Bereichen Steuerung, Datenverarbeitung und -auswertung wird es den amerikanischen Streitkräften ermöglichen, personelle Ressourcen in der Drohnenkriegsführung einzusparen.

Interoperabilität der Systeme

Das Gefechtsfeld der Zukunft wird von *Multi Domain Operations* (MDO)[3] geprägt sein. Bei diesen Operationen werden militärische Aktivitäten in allen Bereichen und Domänen mit nicht unmittelbar militärischen Aktivitäten synchronisiert, um beim Konfliktgegner auf möglichst vielen Ebenen Effekte herbeizuführen und ihn dadurch zu überfordern.[4]

So werden beispielsweise das Informationsumfeld und Lieferketten genutzt, um den Gegner zu schwächen oder zu destabilisieren. Es werden unter anderem über soziale Medien Narrative und Propaganda verbreitet, durch die das Verhalten und die Einstellung der gegnerischen Streitkräfte und der Zivilbevölkerung im Vorfeld militärischer Operationen gezielt beeinflusst werden soll.[5]

Durch die Störung und Blockade von Lieferketten versorgungs- und kriegswichtiger Güter und Rohstoffe soll die Produktionsfähigkeit und Versorgung des Konfliktgegners zumindest kurzfristig beeinträchtigt werden.

Vor allem die Domänen *Cyber* und *Weltraum* werden immer bedeutender – ganz gleich, ob es sich um gezielte Cyberangriffe und Desinformationskampagnen als (militär)taktisches Element, das Abhören oder die Sabotage von Kommunikation oder die aktive Aufklärung über das Ausspionieren von Satelliten- oder Kabelverbindungen handelt. Beide Domänen bilden ein verbindendes Element, führen die weiteren Domänen Land, See und Luft zusammen und erweitern damit die Kombinationsmöglichkeiten. Die Interoperabilität von Systemen wird durch die zunehmende Vernetzung von essenzieller Bedeutung sein.

Eine weitere Entwicklung, die durch die Verknüpfung der Systeme über Cloudlösungen und den Einsatz von KI entsteht, ist die vergrößerte Datenerfassung. Das Schlachtfeld der Zukunft wird datenbasierter. Streitkräfte führen Kameras mit sich, Satelliten oder Drohnen zeichnen etwa Truppenbewegungen auf und generieren so große Datenmengen, die mithilfe von KI und Datenanalysetools sortiert und ausgewertet werden. Dank dieser neuen Dimension der Datenerfassung werden Lagebilder weit präziser, womit sich die Zielgenauigkeit der Waffensysteme erhöhen lässt. Auf dieser Basis steigen die Erfolgschancen militärischer Missionen erheblich, Kollateralschäden lassen sich leichter vermeiden.

Durch die Vielzahl von erfassten Daten lassen sich Informationen gewinnen und über

2 „Replicator: US-Armee will China mit Drohnen überschwemmen“, in: Futurezone.at, 29.08.2023, https://futurezone.at/digital-life/replicator-us-armee-china-drohnen-usa-krieg-schwarm/402573377 [letzter Zugriff: 18.11.2023].

3 Das U.S. Army Training and Doctrine Command hat mit dem „Field Manual 3-0“ (FM 3-0) die Einsatzdoktrin des US-Heeres zu MDOs überarbeitet; vgl. „Multi Domain Operations - U.S. Army veröffentlicht neue Einsatzdoktrin“, in: soldat-und-technik.de, 11.10.2023, https://soldat-und-technik.de/2022/10/streitkraefte/33022/multi-domain-operations-einsatzdoktrin/ [letzter Zugriff: 18.11.2023].

4 NATO: „Multi-Domain Operations in NATO - Explained“, in: act.nato.int, 05.10.2023, www.act.nato.int/article/mdo-in-nato-explained/ [letzter Zugriff: 18.11.2023].

5 Die kognitive Kriegsführung wird von immer mehr Staaten als wesentliches Element künftiger Kriege gesehen, um auf die Moral und Einstellung von Streitkräften und Zivilbevölkerung einzuwirken und die Durchhaltefähigkeit zu beeinträchtigen.

öffentliche Kommunikationskanäle und Social-Media-Plattformen verbreiten. Kriege werden künftig „öffentlicher" ausgetragen. Videos oder Fotos, die in Echtzeit auf TikTok, Instagram, „X" oder anderen Kanälen übertragen werden, geben Einblick in die Geschehnisse auf dem Schlachtfeld. So machen die Internetnutzung und -auswertung, Satellitenaufklärung oder multispektrale Aufklärung das Gefechtsfeld „gläserner", aufgrund der Vielzahl von Parametern und Beeinflussungen jedoch auch komplexer.

Zugleich sind die Informationen fester Bestandteil von kognitiver Kriegsführung. Beispielsweise werden über Visualisierungen Narrative erzeugt, aufgebaut und verbreitet. Ziel ist es vor allem, die Kampfmoral der gegnerischen Truppen durch das Verbreiten von Falschinformationen zu schwächen. Der Informationskrieg wird nicht allein an der Front geführt – die Zivilgesellschaften geraten ebenso ins Visier. Durch die Streuung von Gegennarrativen sollen Verunsicherung und Angst in der Bevölkerung erzeugt werden, um den Rückhalt für Militäreinsätze zu verringern. Diese Informatisierung des Krieges ist unabwendbar.

Verschwimmende Grenzen zwischen Zivil und Militär

Am Beispiel des Cyber- und Informationsraums wird deutlich, dass die Grenzen zwischen Zivil und Militär immer mehr verschwimmen. Private und nichtstaatliche Akteure können etwa durch die Verbreitung von Informationen, wie es in der Ukraine durch Videos von der Front auf TikTok geschehen ist, oder durch Cyberangriffe nichtstaatlicher Hackergruppen unmittelbaren Einfluss auf den Krieg nehmen. Zudem haben einige Geräte, Systeme oder Software Dual-Use-Charakter: Sie können sowohl militärisch als auch zivil genutzt werden. Das Satellitennetzwerk *Starlink* des privatwirtschaftlichen Unternehmens *SpaceX* stellt originär Internetzugänge für die nichtmilitärische Nutzung zur Verfügung. Infolge des russischen Cyberangriffs auf das Satellitennetzwerk *KA-SAT* des US-Anbieters *Viasat* wurde unter anderem die Satellitenkommunikation der ukrainischen Streitkräfte gestört. Elon Musk stellte kurzfristig das Satellitennetzwerk *Starlink* zur Verfügung, um die Satellitenkommunikation der ukrainischen Soldatinnen und Soldaten wiederherzustellen. Somit hatte ein privatwirtschaftliches Unternehmen erheblichen Einfluss auf einen militärischen Konflikt zweier Staaten. Zivile und militärische Sphäre fusionieren zusehends und machen damit eine eindeutige Unterscheidung der beiden Bereiche nur schwer möglich.

Die Automatisierung von Systemen schreitet voran. Anhand der technologischen Entwicklung von Drohnen als unbemannte Flugobjekte, die teilweise bereits KI-gestützt selbstständig navigieren und Ziele erfassen, wird deutlich, wie künftig auch größere Systeme automatisiert zum Einsatz kommen. Die beiden Rüstungsprojekte *Future Combat Air System* (FCAS) und *Main Ground Combat System* (MGCS) geben einen Ausblick auf den möglicherweise zu erreichenden Grad der Vernetzung und Automatisierung. Bei FCAS wird derzeit ein System entwickelt, das (unbemannte) Drohnen, Flugzeuge und Satelliten verknüpft. Es soll das Gefecht der miteinander verbundenen Waffen auf eine neue Ebene heben und unter anderem die Zeit der Abstimmung und Kommunikation zwischen den Systemen erheblich verringern.

Ähnliches gilt für MGCS, bei dem verschiedene bemannte und unbemannte Panzerfahrzeuge miteinander über ein Cloudsystem verbunden sind und in diesem Verbund gemeinschaftlich agieren können. Auch hier wird die Kommunikationszeit zwischen den einzelnen Fahrzeugen erheblich beschleunigt, und

Entscheidungen, die im Hinblick auf ein System getroffen wurden, werden unmittelbar für andere Systeme abgebildet. Aber nicht nur die Kommunikation der verbundenen Systeme wird schneller, sondern auch die Waffen selbst, wie die Entwicklung der neuen Hyperschallwaffentypen zeigt. Die Kriege der Zukunft werden künftig mit weit größerer Dynamik geführt werden. Geschwindigkeit wird zum entscheidenden Faktor, über Sieg oder Niederlage entscheidet die Fähigkeit zur schnellsten Datenerfassung und -verarbeitung.

Neue Fähigkeiten sind gefragt

Der Anteil von Software bei der Kriegsführung wird steigen und das Gefechtsfeld der Zukunft dominieren. Unter dem Stichwort *Software Defined Defense* verbirgt sich ein zentrales Leitprinzip für das Denken und Handeln künftiger Streitkräfte. Durch KI-unterstützte, softwaredominierte, dimensionsübergreifende Systeme werden Fähigkeitszuwächse primär über die Änderung der Software und nicht mehr, wie bisher üblich, durch eine Weiterentwicklung der Hardware erzeugt. Die zunehmende Bedeutung von Software betrifft einzelne Waffensysteme. Analyse-, Planungs- und Entscheidungsprozesse werden durch eine datenzentrierte Architektur optimiert.

Zudem ist ein nutzerzentriertes Design eine nicht zu unterschätzende Frage. So haben die US-Streitkräfte das Steuerungsinterface für Kleindrohnen der Infanterie an den Controller einer X-Box angelehnt. Fast alle jungen Soldatinnen und Soldaten kennen diese Controller aus dem Zivilleben und haben somit kein Problem beim Erlernen der Steuerung. Ein baugleiches Interface soll künftig auch zur Steuerung neuer Großwaffen eingesetzt werden.[6] Nicht die neuesten und stärksten Waffensysteme sind entscheidend für den Vorteil im Gefechtsfeld der Zukunft, sondern das neueste Update.

6 Jared Keller: „The US military will fight the next big war with Xbox-style video game controllers", in: taskandpurpose.com, 22.03.2023, https://taskandpurpose.com/tech-tactics/us-military-video-game-controllers-war/ [letzter Zugriff: 18.11.2023].

7 „Neues Drohnenabwehrsystem für den Feldlagerschutz erfolgreich eingeführt", in: Bundeswehr.de, 15.08.2022, www.bundeswehr.de/de/organisation/ausruestung-baainbw/aktuelles/neues-drohnenabwehrsystem-fuer-den-feldlagerschutz-5475116 [letzter Zugriff: 18.11.2023].

8 Beim Jammen werden Störsignale in einem ausgewählten Frequenzbereich ausgesendet, die die Funkverbindung zur Drohne stören beziehungsweise unterbrechen. Die Drohne stürzt je nach Bauart ab, stoppt die Fortbewegung und verweilt in der Luft oder kehrt zur ihrem Ausgangspunkt zurück.

Diese Entwicklungen verlangen den Streitkräften und ihren Soldatinnen und Soldaten neue Fähigkeiten ab. So wird der Umgang mit Software ein entscheidender Faktor sein. Neben den grundlegenden, erhöhten Anforderungen an das technische Verständnis der Streitkräfte sind auch spezielle IT-Kenntnisse und Fähigkeiten erforderlich. Zur Drohnenabwehr werden etwa Abwehrsysteme gegen unbemannte Luftfahrzeuge (ASUL) eingesetzt.[7] Um das *Jammen* von feindlichen Drohnen[8] zu ermöglichen, senden Radiofrequenz-Peiler und Radarsysteme Daten eines detektierten Luftfahrzeuges an das System, das die Daten mit einer Datenbank zur Identifikation abgleicht. Hierbei kann es zu Störungen kommen, für deren Behebung IT-Spezialisten erforderlich sind.

Die Digitalisierung führt grundsätzlich zu einer Zusammenführung verschiedener Waffengattungen. Demzufolge ist ein größeres Verständnis der Soldatinnen und Soldaten für die Aufgaben, Voraussetzungen und Fähigkeiten ihrer Kameraden der anderen Teilstreitkräfte vonnöten, um im Gefecht der verbundenen Waffen durch die Verknüpfung der verschiedenen Teilstreitkräfte einen Vorteil auf dem Gefechtsfeld zu erzielen.

Die zunehmende Interoperabilität resultiert unter anderem aus einer engeren multinationalen Zusammenarbeit. Dabei wird zwischen der mentalen, der strukturellen und der

materiellen Interoperabilität unterschieden.[9] Auf der mentalen Ebene sind neben einer gemeinsamen Sprache, Terminologie und Doktrin auch gemeinsame Arbeitsverfahren erforderlich. Die Streitkräfte müssen ein gemeinsames Verständnis für die militärischen Aufgaben entwickeln und einheitlich vorgehen. Strukturell bedeutet die Interoperabilität die Anpassung der Kommandostrukturen und die einheitliche Organisation der Stäbe und Verbände sowie die Verfügbarkeit von Kommunikations- und Informationssystemen. In materieller Hinsicht gilt das für die Kompatibilität der Ausrüstung und die logistische Zusammenarbeit. Für die Streitkräfte bedeutet dies konkret, die sprachlichen Fertigkeiten auszubauen und eine Offenheit gegenüber anderen Prozessen, Abläufen und Verfahren zu entwickeln, sodass multinationale Kooperationen einfacher und schneller möglich sind.

Für Soldatinnen und Soldaten wird infolge der Informatisierung die digitale Ausbildung *(digital literacy)* bedeutsamer. Neben der eigenen Rolle im Informationsumfeld als Akteur (etwa durch die Übermittlung von Informationen und Narrativen) und als wesentlicher Bestandteil von strategischer Kommunikation ist auch die Auseinandersetzung mit den Potenzialen und Risiken von Desinformation, Deep Fakes und kognitiver Kriegsführung anderer Staaten unerlässlich. Immer mehr bemannte sowie unbemannte Systeme werden durch Künstliche Intelligenz unterstützt und Soldatinnen und Soldaten einzelne Aufgaben abgenommen. Ihnen wird ein größerer zeitlicher Spielraum für wesentliche Entscheidungsprozesse gewährt.

An die neue Schnelllebigkeit auf dem Gefechtsfeld müssen sich die Soldaten ebenso gewöhnen wie an die künftige Multinationalität. Zwar werden die Kriege der Zukunft immer mehr von Software und neuer Technologie dominiert, doch werden auch im Rahmen der Entwicklung die Anwendungen auf die Soldatinnen und Soldaten zentriert werden müssen. Es wird künftig nicht nur IT-Spezialisten und Informatiker erfordern, um auf dem Gefechtsfeld der Zukunft zu bestehen. Notwendig sind jedoch mehr Cyberstreiter, die die neuen Technologien beherrschen und sie einzusetzen wissen.

9 „Interoperabilität: Gemeinsames Handeln für eine sichere Zukunft“, in: Bundeswehr.de, 22.06.2023, www.bundeswehr.de/de/organisation/luftwaffe/aktuelles/-interoperabilitaet-gemeinsames-handeln-5639252 [letzter Zugriff: 18.11.2023].