

Kriegsführung im Cyberzeitalter

Zusammenfassung

Neue strategische Waffen, neue Kriegskonzepte und dynamische geopolitische Konstellationen verändern die Art und Weise der Kriegsführung im Cyberzeitalter. Vor allem intelligenten Maschinen, die schneller, ausdauernder und oft kostengünstiger als Menschen sind, wird hohes Zukunftspotenzial zugeschrieben. Gerade die Überlegenheit digitaler und autonomer Waffentechnologien wird zum Gamechanger in militärischen Konfrontationen und bedingt neue Bedrohungslagen und Herausforderungen.

Überblick zum Thema

Das schwedische Universitätsdepartment für Friedens- und Konfliktforschung stellt im Rahmen des „Uppsala Conflict Data Program (UCDP)“ seit 40 Jahren systematisch Daten zu organisierter Gewalt, bewaffneten Konflikten und Bürgerkriegen bereit.¹ Als militärischer Konflikt wird dabei ein Ereignis mit mindestens 25 Toten, verursacht durch staatliche Gewalt oder bewaffnete Gruppen, verstanden. Hotspots für solche Ereignisse sind in den letzten Jahren Afghanistan, Jemen, Syrien und Irak sowie Somalia, die Sahel-Region und Nigeria. Die Zahl der zwischenstaatlichen Kriege ist gesunken, während die Zahl der innerstaatlichen Konflikte (Bürgerkriege) zugenommen hat. Die meisten Opfer fordern innerstaatliche Konflikte mit ausländischer Beteiligung (z. B. in Syrien, der zentralafrikanischen Republik oder Myanmar). Die Hauptakteure im Kriegsgeschehen sind die militärischen Großmächte USA, Großbritannien, China, Russland und Frankreich, die sich bereits auf die Zukunft des Kriegs vorbereiten. Während Großbritannien eine Zukunft anvisiert, in der ein Viertel aller SoldatInnen bis 2030 durch Roboter ersetzt sein wird,² will Russland bis 2025 bereits ein Drittel substituiert haben.³ Länder, in denen die Entwicklung von Robotern und KI (siehe [Sicherheits-Robotik](#)) forschungsstrategische Priorität ist, haben auch hohe Rüstungsausgaben. Im Jahr 2020 lagen die USA mit 738 Milliarden US-Dollar, China mit 193 Milliarden US-Dollar und Russland mit 60 Milliarden US-Dollar an der Ausgaben Spitze. In Europa liegen Großbritannien und Frankreich voran.⁴

*Mehr innerstaatliche,
bewaffnete Konflikte*

*Zukunftstrend:
Roboterarmee*

*Forschungs- und
Rüstungsausgaben*

2021 wurde ein iranischer Nuklearwissenschaftler von einem sogenannten Killerroboter – in diesem Fall von einer ferngesteuerten bewaffneten Drohne – getötet.⁵ Der Tötungsbefehl wurde der Maschine diesmal noch von einem Angehörigen des Militärs, der über 1.000 km vom Attentat ent-

*Neue KI-
Waffentechnologien*

¹ pcr.uu.se/research/UCDP/.

² the-decoder.de/ki-im-militaer-die-britische-armee-plant-mit-robotersoldaten.

³ publikationen.bibliothek.kit.edu/1000127160.

⁴ arte.tv/de/videos/103960-009-A/mit-offenen-karten/.

⁵ futurezone.at/digital-life/iran-kernphysiker-killer-roboter-anschlag-drohne-ki/401741343.

fernt war, gegeben. Doch eine Zukunft, in der autonome Waffen- und Kriegssysteme eingesetzt werden, die schneller, ausdauernder und kostengünstiger als Menschen sind und ohne deren Zutun töten, rückt näher. Aktuell sind bereits Robo-Maultiere für den Lastentransport und Minenräumroboter, sowie autonome Panzerwagen im Einsatz,⁶ die zukünftig miteinander kommunizieren und sich gegenseitig reparieren sollen. Flug- und Unterwasserdrohnen (siehe Thema [Lieferdrohnen](#)) werden seit längerem aus Kostengründen militärisch genutzt. Neuer sind sogenannte Mikro-Drohnen im militärischen Nachrichtenwesen, die nur einige Zentimeter breit sind, zu Hunderten abgeworfen werden und in Schwarmformation autonom operieren. Welche Länder verfügen über militärische Drohnen? 102 Staaten haben Militärdrohnen für Aufklärungszwecke (darunter Österreich⁷), 40 Staaten besitzen bewaffnete Drohnen und sechs Länder exportieren Drohnen (USA, Russland, China, Israel, VAE, Türkei).⁸

**Zunehmende Autonomie
von Waffensystemen**

Seit 2001 haben immer mehr Einsätze und Angriffe mit Drohnen stattgefunden, aber erst 2019 haben Kampfdrohnen im Libyen-Krieg zum ersten Mal autonom angegriffen.⁹ Bislang haben Militärangehörige die Verantwortung für ihre Waffen und ihre Übergriffe getragen. Was passiert, wenn zukünftig Maschinen die Entscheidung treffen anzugreifen? Welche technologiebezogenen und gesellschaftsrelevanten Gefahren gehen damit einher?

**Sicherheitsökonomische
und dystopische
Anwendungsszenarien**

Während sicherheitsökonomische Zukunftsvisionen den strategischen Vorteil durch schnellere und intelligentere Kriegssysteme, die Erhöhung der Sicherheit von SoldatInnen und der Bevölkerung sowie die Kostenreduktion durch den Einsatz von Drohnen, Robotern und KI in den Vordergrund stellen, betonen dystopische Szenarien technologische Schwachstellen und das hohe Missbrauchspotenzial. Roboter und KI-basierte Kriegssysteme können – wie jeder andere Computer auch – gehackt, verändert und für unlautere Zwecke genutzt werden.¹⁰ Außerdem unterliegen sie den gleichen Herausforderungen wie allgemeine KI-Anwendungen: der Black Box des maschinellen Lernens, d. h. der fehlenden Möglichkeit, die Entscheidungen einer KI ausreichend nachzuvollziehen, sowie Verzerrungen, die durch schlecht ausgewählte Trainingsbeispiele (Lerndaten) entstehen und zu Fehlentscheidungen führen können. Ausschlaggebend für die internationale Diskussion ist das „Human-in-the-loop“-Prinzip, das die Notwendigkeit menschlicher Kontrolle bzw. Interaktion in KI-basierten Entscheidungsmodellen betont.¹¹ In der Forschung gibt es bereits Vorschläge für eine

**Human-in-the-loop
Prinzip**

⁶ [web.archive.org/web/20070710104756/http://www.dtic.mil/whs/directives/correspdf/500059m.pdf](http://www.dtic.mil/whs/directives/correspdf/500059m.pdf).

⁷ rechnungshof.gv.at/rh/home/home/004.667_Drohnen_Einsatz_Bundesheer.pdf.

⁸ arte.tv/de/videos/103960-009-A/mit-offenen-karten/.

⁹ Dabei handelte es sich um türkische Kampfdrohnen, die im Libyen-Konflikt der Armee in Tripolis halfen, die Armee von General Haftar zurückzudrängen.

¹⁰ In Syrien kamen zivile Drohnen zum Einsatz, die umgebaut und mit Granatwerfern ausgestattet wurden, siehe: [bellingcat.com/news/mena/2017/02/10/death-drone-bombs-caliphate/](https://www.bellingcat.com/news/mena/2017/02/10/death-drone-bombs-caliphate/).

¹¹ [web.archive.org/web/20070710104756/http://www.dtic.mil/whs/directives/correspdf/500059m.pdf](http://www.dtic.mil/whs/directives/correspdf/500059m.pdf).

verantwortungsvolle und menschenzentrierte militärische Nutzung von KI-Technologie, siehe z. B. Boulanin et al. (2020).

Kampagnen gegen den Einsatz von Killerrobotern kritisieren das neue Wettrüsten weltweit und fordern ein Verbot.¹² Das EU-Parlament und 120 Staaten der blockfreien Bewegung¹³ haben sich dieser Forderung nach einem präventiven Verbot von Killerrobotern angeschlossen. Seit sieben Jahren wird international über das Verbot autonomer Waffensysteme debattiert,¹⁴ aber zwölf gewichtige Staaten verzögern den Aushandlungsprozess, und Russland nimmt gar nicht erst an den Verhandlungen teil. Andere Länder wie z. B. Frankreich und Deutschland sind für eine kontrollierte, rechtlich nicht bindende Eindämmung.

*Verbot von
Killerrobotern?*

Doch alle Maßnahmen, die auf einen sicheren Einsatz von KI abzielen, könnten nicht verhindern, dass die Technologie in falsche Hände gerät. Daher werden Kriegsführungsstrategien an neue Bedrohungslagen, wie z. B. hybride Bedrohungen („hybrid threats“), angepasst. Sie sind dadurch definiert, dass sie Begriffe wie Freund/Feind oder wahr/falsch verwischen und Mehrdeutigkeit schaffen (Cullen et al. 2021). Ein Beispiel sind gezielte und umfassende Desinformationskampagnen, die auf politische Destabilisierung zielen, aber auch Cyberangriffe, Spionage, politische Subversion, Sabotage, u. a. zählen dazu. In Verbindung mit diesen neuen Bedrohungen steht auch der Begriff der hybriden Kriegsführung („hybrid warfare“). Er umfasst das Verschwimmen der Kriegsformen und die Verwischung der Fragen „Wer kämpft?“ und „Welche Technologien kommen zum Einsatz?“ (Hoffmann 2007). Wie der Cyberangriff „Stuxnet“ auf industrielle Kontrollsysteme u. a. eines iranischen Atomkraftwerks beispielhaft zeigt, überschneiden sich die Konzepte von Cyberkriegsführung¹⁵ („cyberwarfare“) und hybrider Kriegsführung.¹⁶ Das aktuellere Kriegskonzept der Mosaik-Kriegsführung („mosaic warfare“) stellt Komplexität in den Mittelpunkt und versteht sie als strategische Waffe. Wie Keramikfliesen in einem Mosaik werden die einzelnen Kriegsführungssysteme wie z. B. Drohnen, Flugzeuge und Cyberangriffe, über eine Plattform zu einer größeren integrierten Mission zusammengefügt. Die Idee dahinter ist, den Feind mit Hilfe von vielzähligen KI-basierten Waffen- und Sensorsystemen, die schnell reagieren können, zu überwältigen (Zhang et al. 2020).¹⁷ Zukünftige Gefahren sehen ExpertInnen in der hohen Effizienz von Mosaik-Kriegsführung,

*Neue
Bedrohungslagen*

*Neue
Kriegskonzepte*

Mosaik-Kriegsführung

¹² stopkillerrobots.org/; <https://krcaustria.at/>.

¹³ Internationale Organisation von Staaten, die nach dem zweiten Weltkrieg während des Ost-West-Konflikts militärisch neutral blieben und unter denen sich keine großen Militärmächte befinden.

¹⁴ derstandard.at/story/2000130084550/warum-killerroboter-verboten-werden-sollten-ehe-sie-eingesetzt-werden.

¹⁵ Es gibt Diskussionen darüber, was Cyberkriegsführung genau ist, siehe z. B. nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html.

¹⁶ Es wird vermutet, dass die aufwändige Attacke aufgrund ihrer Komplexität und hohen Kosten nur ein Nationalstaat durchführen konnte, siehe archive.org/details/w32_stuxnet_dossier.

¹⁷ arpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosaic-warfare.

die zu einer sicheren Gewinnaussicht führen kann und damit hohes disruptives Potenzial v. a. aus geopolitischer Perspektive hat.

Relevanz des Themas für das Parlament und für Österreich

Obwohl KI bereits im zivilen und militärischen Bereich eingesetzt wird, dürfte sich ihre Anwendung zur Entscheidungsunterstützung in einem militärischen Kontext erst mittelfristig, in etwa fünf bis zehn Jahren, stärker auswirken (Bordin et al. 2020). Gerade deshalb gilt es, das Risiko neuer humanitärer Katastrophen mit all ihren Folgewirkungen (Zivile Opfer, Armut, Migration) oder die zunehmend asymmetrische Kriegsführung, die zu langanhaltenden Konflikten und nachhaltiger Beeinträchtigung von globalen Beziehungen führen kann, ausführlich zu bedenken. Auf Ebene der europäischen Verteidigungspolitik zeichnen sich zwei Treiber ab, die das Thema für Österreich relevant machen.¹⁸ Einerseits ist das der Wunsch¹⁹ nach einer stärkeren gestalterischen Rolle in der globalen Debatte zur militärischen Nutzung von KI,²⁰ andererseits das Bestreben eine größere Interoperabilität zwischen den EU-Streitkräften zu fördern und die europäische Zusammenarbeit in der militärischen Forschung und Entwicklung zu verbessern, was für Mitgliedsstaaten auch wirtschaftliche Vorteile haben könnte. Die aktive Beteiligung Österreichs an der Forderung nach einem internationalen Verbot von Killerrobotern bietet Orientierung und eine stabile Ausgangsbasis für die wirtschaftliche Positionierung.

Vorschlag weiteres Vorgehen

Es bietet sich ein Foresight-Prozess zur Entwicklung einer europäischen Zukunftsvision für die verantwortungsvolle militärische Nutzung von KI an, an den eine Österreich-spezifische Vorausschau angedockt werden könnte, die die Potenziale Österreichs weiter exploriert. Auch die Frage nach ethischen, sozialen und rechtlichen Rahmenbedingungen, die zukünftig diesen verantwortungsvollen Umgang mit KI ermöglichen sollen, könnte in einer Vorausschau beantwortet werden. Hier bietet sich an zu untersuchen, inwieweit Dual-Use-Handelskontrollen zur Transparenz des internationalen Handels mit Waffen- und Kriegssystemen beitragen können, siehe z. B. Bromley & Brockmann (2021), und welche Innovationen zukünftig die Nachvollziehbarkeit militärischer Entscheidungen in KI-basierter Kriegsführung erhöhen könnten.

¹⁸ parlament.gv.at/PAKT/PR/JAHR_2021/PK0193/index.shtml.

¹⁹ Dieser Wunsch ergibt sich vor allem aus den Erfahrungen und bisherigen Aktivitäten der EU in Hinblick auf die ethische und verantwortungsvolle Nutzung von KI im zivilen Bereich (siehe z. B. Berichte und Positionspapiere der High-Level Expert Group on AI und der European AI Alliance) und dem Potenzial einer europäischen Vision für die verantwortungsvolle militärische Nutzung von KI.

²⁰ So hat Österreich zusammen mit Panama im UNO-Menschenrechtsrat eine Resolution zu autonomen Waffensystemen eingebracht, die mit Konsens verabschiedet wurde und die festhält, dass der Einsatz letaler autonomer Waffensysteme ausreichender menschlicher Kontrolle zu unterliegen hat, siehe orf.at/stories/3288605.

Zitierte Literatur

- Bordin, G., Hristova, M. und Luque Perez, E., 2020, JRC horizon scanning on dual-use civil and military research, Luxembourg: Publications Office of the European Union.
- Boulanin, V. et al. 2020, Responsible Military Use of Artificial Intelligence; in Reihe: SIPRI Publication, Solna, Sweden: SIPRI.
- Bromley, M. und Brockmann, K., 2021, Implementing the 2021 Recast of the EU Dual-use Regulation: Challenges and Opportunities; in Reihe: SIPRI Publications: EUNPDC.
- Cullen, P. et al., 2021, The landscape of Hybrid Threats: A Conceptual Model (Public Version), in: Giannopoulos, G. et al. (Hg.), Luxembourg: Publications Office of the European Union.
- Hoffmann, F. G., 2007, Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington: Potomac Institute for Policy Studies.
- Zhang, N., Zhu, X. und Gou, Y., 2020, The role of artificial intelligence and autonomous systems in the decision-making center of the US mosaic war, 2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI), 4-6 Dec. 2020.