Ralph Thiele *Hrsg.*

Hybride Kriegsführung

Zukunft und Technologien

Springer VS

Hybride Kriegsführung

Ralph Thiele
Hrsg.

Hybride Kriegsführung

Zukunft und Technologien

Springer VS

Hrsg.
Ralph Thiele
StratByrd Consulting
Nickenich, Deutschland

Dieses Buch ist eine Übersetzung des Originals in Englisch „Hybrid Warfare“ von Thiele, Ralph, publiziert durch Springer Fachmedien Wiesbaden GmbH im Jahr 2021. Die Übersetzung erfolgte mit Hilfe von künstlicher Intelligenz (maschinelle Übersetzung durch den Dienst DeepL.com). Eine anschließende Überarbeitung im Satzbetrieb erfolgte vor allem in inhaltlicher Hinsicht, so dass sich das Buch stilistisch anders lesen wird als eine herkömmliche Übersetzung. Springer Nature arbeitet kontinuierlich an der Weiterentwicklung von Werkzeugen für die Produktion von Büchern und an den damit verbundenen Technologien zur Unterstützung der Autoren.

ISBN 978-3-658-40518-2 ISBN 978-3-658-40519-9 (eBook)
https://doi.org/10.1007/978-3-658-40519-9

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer VS

Planung/Lektorat: Jan Treibel
Springer VS ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Im Zusammenhang mit internationalen Spannungen oder Konflikten niedriger Intensität hat der Begriff der hybriden Kriegsführung zunehmend an Bedeutung gewonnen. Auch wenn sich eine tragfähige Definition dieses Begriffs international noch nicht durchgesetzt hat, macht dieses Buch einen bemerkenswerten Vorschlag in dieser Hinsicht. Es trägt nicht nur dazu bei, das breite Spektrum an Mitteln der hybriden Kriegsführung zu beleuchten, sondern zeigt auch auf, wie diese neue Form des Konflikts die Art des Krieges in den nächsten Jahrzehnten verändern wird.

Hybride Kriege haben ihren Ursprung oft in Konflikten aufgrund von Überbevölkerung, religiösen Differenzen, dem Kampf ethnischer und religiöser Minderheiten um Selbstbestimmung und Unabhängigkeit oder im Zusammenhang mit der Zerstörung der natürlichen Lebensgrundlagen. Solche Konflikte sind auch der Nährboden für den Kampf der Großmächte um Einflusszonen und für Stellvertreterkriege der Regionalmächte um regionale Vorherrschaft.

Der russische Generalstabschef Valery Gerasimov gilt als geistiger Vater des Konzepts der hybriden Kriegsführung. Bereits 2013 wies er darauf hin, dass Aufstände und interne Konflikte die Initialzündung für hybride Kriege sind. Diese Kriegsführung zeichnet sich durch ein breites Spektrum an militärischen, paramilitärischen und wirtschaftlichen Maßnahmen sowie den offensiven Einsatz von Informationstechnologie aus. Seine entsprechenden konzeptionellen Überlegungen sind als *Gerasimow-Doktrin* bekannt geworden. Die Anwendung der *Gerasimow-Doktrin* ist in den Konflikten in Nordafrika, im Nahen und Mittleren Osten und in der Ukraine zu beobachten.

Aufgrund der dramatischen Fortschritte in der Informationstechnologie hat sich der Schwerpunkt der hybriden Kriegsführung in den letzten Jahren auf den Einsatz von Cyberangriffen verlagert. Cyberangriffe in Verbindung mit aufkommenden

und disruptiven Technologien verleihen der hybriden Kriegsführung eine neue Qualität. Globalisierung, Digitalisierung und fortschrittliche Technologien haben den Lebensstandard insbesondere in den Vereinigten Staaten und Europa verbessert. Gleichzeitig sind neue Schwachstellen in offenen und demokratischen Gesellschaften entstanden. Diese Schwachstellen werden von den Gegnern adressiert und gezielt ausgenutzt.

Mit diesen neuen Möglichkeiten ist der hybride Krieg zu einem wesentlichen Instrument in Konflikten zwischen den Großmächten geworden. Mit der Verschärfung der Rivalität zwischen diesen Mächten, nämlich den Vereinigten Staaten, China und Russland, hat sich die Anwendung des hybriden Krieges in den letzten Jahren intensiviert. Die exponentiellen Fortschritte in der Digitalisierung kommen vor allem China und den Vereinigten Staaten zugute. Aber auch Russland hat erhebliche Fortschritte gemacht. Die hybride Kriegsführung hat den großen Vorteil, dass sie unterhalb der Schwelle des offenen Krieges eingesetzt werden kann, da die Maßnahmen hinsichtlich der eingesetzten Mittel, der Intensität und des Ausmaßes des Schadens, der der anderen Seite zugefügt werden soll, an die jeweilige Situation angepasst werden können.

Wie wichtig diese Entwicklung ist, zeigt die Tatsache, dass die Vereinigten Staaten Russland offen beschuldigen, sich mit Cyber-Angriffen zu einer Vielzahl von US-Regierungsstellen Zutritt verschafft zu haben und die NATO durch Einschüchterung und aktive Maßnahmen zu untergraben. Nur wenige Tage nach seinem Amtsantritt hat US-Präsident Biden den Stellenwert von Cyber-Angelegenheiten in der amerikanischen Regierung erhöht, indem er den ersten stellvertretenden nationalen Sicherheitsberater für Cyber und neue Technologien ernannt hat. Darüber hinaus startete er eine dringende Initiative zur Verbesserung der Fähigkeiten, der Bereitschaft und der Widerstandsfähigkeit im Cyberspace.

Massive Angriffe auf politische Systeme, Regierungen, Wirtschaft, Verkehr, Energie und Informationssysteme offener Gesellschaften können ein Land oder ein Bündnis teilweise oder vollständig lahmlegen. Es handelt sich um einen nicht erklärten Krieg, und der Feind kann nicht – oder zumindest nicht sofort – identifiziert werden. Der Angriff kann begrenzt und selektiv sein, aber er kann jederzeit ausgeweitet und verstärkt werden. Eine Antwort in Form eines Angriffs ist jedoch keine wirksame Option.

Eine hybride Kriegsführung kann langfristig erfolgreicher sein als der Einsatz von Streitkräften. In den letzten Jahrzehnten war das strategische Prinzip der Abschreckung ein fester Bestandteil der westlichen Strategie. Abschreckung funktioniert, wenn ein potenzieller Angreifer größere Nachteile als mögliche Vorteile aus einem Konflikt zu erwarten hat. In der hybriden Kriegsführung funktioniert Abschreckung nicht. Daher ist es wichtig, in neue Technologien zu investieren, um die

Wirtschaftskraft und damit die Widerstandsfähigkeit vor allem der Europäischen Union und der NATO-Mitgliedstaaten zu stärken. Es gibt eine Fülle von aufkommenden und disruptiven Technologien. Die NATO betrachtet Daten, künstliche Intelligenz, Autonomie, Weltraumtechnologien und Hyperschall als vorwiegend disruptive Technologien, während Quantencomputer, Biotechnologie und fortgeschrittene Werkstoffe eher im Entstehen begriffen sind, wobei letztere mehr Zeit benötigen, bevor ihre disruptive Wirkung auf die militärischen Fähigkeiten spürbar wird.

Neue und disruptive Technologien ermöglichen eine hybride Kriegsführung mit dem Ziel, bereits entscheidende Vorteile gegenüber einem Gegner zu erzielen, bevor militärische Kampfhandlungen im offenen Krieg begonnen haben. Sie schaffen auch die notwendigen Voraussetzungen, um ein umfassendes Situationsbewusstsein und Informationsüberlegenheit zu erreichen. Durch den gezielten Einsatz von Cyber- und Informationstechnologien zur Täuschung und Verwirrung bis hin zur Ausschaltung der gegnerischen Führungs- und Informationssysteme kann der Gegner in der Anfangsphase eines Krieges so weit geschwächt werden, dass die nachfolgenden militärischen Maßnahmen mit deutlich geringerem Risiko und höheren Erfolgschancen durchgeführt werden können.

In allen Kriegen haben exponentielle technologische Entwicklungen eine wichtige Rolle gespielt, wenn sie mindestens einen der strategischen Faktoren Zeit, Raum und Macht zugunsten einer Kriegspartei entscheidend verändert haben. Im 20. Jahrhundert waren es die Flugzeuge, die Zeit und Raum veränderten und mit dem Ziel eingesetzt wurden, die industrielle und wirtschaftliche Basis des Gegners zu zerstören. Einen noch größeren Einfluss hatte die Erfindung der Raketen, die aufgrund ihrer interkontinentalen Reichweite und als Trägersystem für nukleare Sprengköpfe mit immenser Zerstörungskraft die Strategie der Abschreckung durch Zweitschlagfähigkeit ermöglichten. So wirksam diese Strategie bis heute ist, so moralisch fragwürdig ist sie.

Robotik, künstliche Intelligenz, autonome Systeme und Hyperschallwaffensysteme werden in hochintensiven militärischen Konflikten der Zukunft entscheidend sein. Während Raketen einer ballistischen Flugbahn folgen und daher von Frühwarnsystemen entdeckt und damit auch bekämpft werden können, sind Hyperschallwaffensysteme manövrierfähig und können entweder entsprechend programmiert werden oder spontan ihren Kurs ändern. Sie können nukleare Sprengköpfe tragen oder konventionell ihre Ziele mit der kinetischen Energie ihrer Geschwindigkeit zerstören. Aufgrund ihrer hohen Geschwindigkeit, ihrer Manövrierfähigkeit und ihrer geringen Flughöhe sind Hyperschallwaffensysteme schwer aufzuspüren und bisher praktisch nicht zu verteidigen.

Ralph Thiele hat mit diesem Buch ein Standardwerk zur hybriden Kriegsführung geschaffen. Es zeigt umfassend auf, wie politische Rivalitäten und Konflikte in Zukunft unter Einsatz einer Vielzahl von neuen und disruptiven Technologien ausgetragen werden. Der Autor zeigt auch auf, wie sich offene Gesellschaften, insbesondere westliche Demokratien, gegen hybride Angriffe schützen und aktiv verteidigen können. Die Europäische Union und die NATO sollten diese Vorschläge so schnell wie möglich aufgreifen. Für Europa ist dies eine entscheidende Voraussetzung für eine Politik der politischen, wirtschaftlichen und militärischen Selbstbehauptung in der neuen Machtarithmetik des globalen Wettstreits der Großmächte.

General (a.D.) Harald Kujat

Vorwort

Die hybride Kriegsführung ist ein altes Phänomen, das heute durch neue technologische Entwicklungen erheblich gestärkt wird. Neue Technologien mit ihrem disruptiven Potenzial haben eine katalytische Wirkung auf hybride Mittel, Methoden, Taktiken und Strategien. Sie verbessern die Ausgangsbedingungen für hybride Aktionen, erweitern das Arsenal hybrider Akteure und tragen so dazu bei, die Reichweite ihrer Aktivitäten sowie ihre Erfolgsaussichten zu erhöhen. Bedenklich ist, dass sie vor allem offensive Optionen bieten. Gleichzeitig können neue technologische Entwicklungen Optionen bieten, um hybride Angriffe besser zu erkennen, zu verstehen, abzuwehren und zu kontern. Vor allem aber machen neue technologische Trends die Technologie zunehmend zu einem „Schlachtfeld" für die hybride Konfrontation als solche. Vor diesem Hintergrund stellt die Technologie eine zusätzliche Domäne und eine Möglichkeit für hybride Akteure dar, den „Kampfplatz" horizontal auszuweiten. Der technologische Bereich kann sogar zum Gravitationszentrum einer hybriden Konfrontation werden. Um hybriden Gegnern vorzubeugen, sie abzuwehren und – falls erforderlich – zu kontern und zu überlisten, ist es daher für politische, zivile und militärische Führungskräfte und Entscheidungsträger sowie für Industrie und Wissenschaft wichtig, ein gemeinsames und umfassendes Verständnis der Auswirkungen neuer Technologien im Kontext hybrider Bedrohungen/Kriegsführung zu entwickeln.

Vor diesem Hintergrund haben das Europäische Exzellenzzentrum für die Bekämpfung hybrider Bedrohungen (Hybrid CoE) und seine Interessengemeinschaft

für Strategie und Verteidigung (COI S&D)[1] das Projekt „Hybrid Warfare“ initiiert und durchgeführt: Future & Technologies (HYFUTEC) mit dem vorrangigen Ziel, westlichen politischen Entscheidungsträgern Empfehlungen für die entscheidende Schnittstelle zwischen Technologie und dem Komplex hybrider Bedrohungen/Kriegsführung zu geben. Das Projekt zielt darauf ab, das Bewusstsein und das Verständnis für die Auswirkungen neuer Technologien und deren Störungspotenzial im Kontext hybrider Bedrohungen/Kriegsführung zu verbessern. Dies wird als besonders wichtig für politische, zivile und militärische Führungskräfte, Entscheidungsträger und konzeptionelle Planer sowie für die Industrie und den akademischen Bereich erachtet. In diesem Sinne bietet HYFUTEC eine „Brückenfunktion“ zwischen der technologischen Revolution auf der einen Seite und der „Welt der hybriden Bedrohungen/Kriegsführung“ auf der anderen Seite, mit „Übersetzungsleistungen“ in beide Richtungen.

Vier Module haben das Projekt strukturiert: Erstens ein breit angelegter „Zukunfts- und Technologie-Horizontscan“, zweitens die jeweilige „Bewertung der hybriden Kriegsführung und damit verbundener Strategien“ auf der Grundlage eigener konzeptioneller Arbeiten, drittens ein spezieller Fokus auf „ausgewählte, besonders relevante Trends“ und schließlich die Ableitung von „sicherheits-

[1] Die im August 2018 gegründete, von Deutschland geleitete Interessengemeinschaft Strategie & Verteidigung befasst sich mit hybrider Kriegsführung, damit verbundenen Strategien und den daraus resultierenden Implikationen für Sicherheitspolitik, Militär und Verteidigung. Sie zielt darauf ab, das Wesen und die Natur hybrider Kriegsführung sowie die Logik und die Muster hybrider Strategien aufzudecken, um einen soliden konzeptionellen/analytischen Rahmen als Grundlage für die Bewertung aktueller und zukünftiger hybrider Kriegsführungssituationen und ihrer praktischen Auswirkungen zu entwickeln. Die COI S&D verfolgt einen interdisziplinären, sowohl praktischen als auch akademischen Ansatz, der empirische Erkenntnisse mit Kriegs- und Strategietheorie verbindet. Um die verschiedenen Blickwinkel und Perspektiven des Themas abzudecken, verfolgt und integriert die COI S&D fünf miteinander verbundene Lines of Effort (LoE): 1) Strategie, 2) Krieg, 3) Fallstudien, 4) Technologie und 5) Frieden. HYFUTEC ist einer von vier übergreifenden Arbeitsbereichen, die derzeit die Bemühungen von COI S&D anführen. Das übergreifende Ziel der COI S&D ist es, zur Bildung eines gemeinsamen und umfassenden Verständnisses und Urteilsvermögens der Teilnehmerstaaten, der EU und der NATO in Bezug auf den Komplex der hybriden Bedrohungen/Konflikte/Kriegsführung beizutragen, als Voraussetzung für ein verbessertes Situationsbewusstsein sowie für ein gemeinsames und umfassendes Vorgehen bei der Verteidigung und Reaktion.

politischen, militärischen und verteidigungspolitischen Implikationen“ für EU, NATO und Mitgliedstaaten. Es wurde 2019 mit einer Reihe von Veranstaltungen in Helsinki, Berlin, Wien und Stockholm gestartet. Im Rahmen des breit angelegten Zukunfts- und Technologie-Horizontscannings hat das Projekt 19 technologische Trends mit dringenden und tiefgreifenden Auswirkungen auf die Entwicklung von hybriden Bedrohungen, Konflikten und Kriegsführung identifiziert. In den Jahren 2020 und 2021 wurde HYFUTEC an der Baltischen Verteidigungsakademie in Tartu erfolgreich als Bildungsinstrument getestet. Die wichtigsten Ergebnisse des Projekts wurden auf dem HYFUTEC-Online-Symposium „Mind the Gaps“ im September 2020 vorgestellt und diskutiert. Dieses Symposium markierte den Abschluss der HYFUTEC-Projektphase und den Übergang zu HYFUTEC als fortgesetzter Arbeitsstrang des COI Strategy & Defence.

Im Laufe des Projekts tauschten Experten und Praktiker aus den verschiedensten Bereichen, darunter Kanzlerämter, Verteidigungs-, Innen- und Außenministerien, Diplomaten, Nachrichtendienste, andere staatliche und internationale Agenturen wie die Europäische Verteidigungsagentur (EDA) und die Gemeinsame Forschungsstelle (GFS), weitere nationale und internationale Forschungszentren, Denkfabriken, Hochschulen und der Privatsektor Erkenntnisse, Beiträge, Präsentationen und Informationen aus und diskutierten die Ergebnisse in einer Reihe von Workshops in ganz Europa. Durch ihren Wissensschatz wurde sichergestellt, dass die Ergebnisse auf einer fundierten und umfassenden Expertise beruhen. Insgesamt versammelte das HYFUTEC-Netzwerk mehr als 260 Experten aus Wissenschaft und Industrie aus 27 Teilnehmerstaaten sowie Vertreter von NATO- und EU-Institutionen.

Diese Monographie spiegelt die Ergebnisse des Projekts *Hybrid Warfare: Future & Technologies, das* vom Europäischen Exzellenzzentrum für die Bekämpfung hybrider Bedrohungen (Hybrid COE) und seiner Interessengemeinschaft Strategie und Verteidigung (COI S&D) in enger Zusammenarbeit mit StratByrd Consulting von Dezember 2018 bis September 2020 in Auftrag gegeben und geleitet wurde. Es wirft einen Blick auf den breiteren Kontext der hybriden Kriegsführung auf der Grundlage konzeptioneller Überlegungen, wie sie in Kapitel zwei „*Einführung in die hybride Kriegsführung*“ dargelegt sind. Es identifiziert mögliche hybride Akteure und deren Ansätze. Er hebt die Rolle der Digitalisierung hervor und zeigt auf, wie sich die sich entwickelnden Revolutionen in militärischen Angelegenheiten auf den Kontext der hybriden Bedrohungen/Kriegsführung auswirken können – und sich wahrscheinlich weiter entwickeln werden.

Ein Zukunfts- und Technologiehorizontscan liefert eine breite Perspektive auf relevante Trends, Störpotenzial, Bedrohungen, Risiken und Akteure, den Einsatz von Gewalt und Kriegsführungsoptionen sowie das Potenzial für Sicherheit und Verteidigung. Besonders relevante Trends werden bei 19 ausgewählten Technologien verfolgt und im Hinblick auf die hybride Kriegsführung und damit verbundene Strategien bewertet. Fünf dieser Technologien – der Technologiestandard der fünften Generation für Mobilfunknetze (5G), künstliche Intelligenz (KI), autonome Systeme, Quantenwissenschaften und neue Entwicklungen in der Raumfahrt – werden zusätzlich in den Anhängen ausführlicher behandelt. Die Bewertung der hybriden Kriegsführung und der damit verbundenen Strategien legt den Schwerpunkt auf konzeptionelle Perspektiven des Manövrierens im Raum der hybriden Konflikte/Kriegsführung, die Aktivitäten in operativen und strategischen Bereichen wie Land, See, Luft, Weltraum und Cyber umfassen. Es werden die Auswirkungen auf Sicherheitspolitik, Militär und Verteidigung analysiert. Es werden konzeptionelle, technologische und organisatorische Empfehlungen abgeleitet, um in der NATO, der EU und den Mitgliedstaaten die Sichtweise der Regierungen, der Wissenschaft und des privaten Sektors zu Fragen der hybriden Kriegsführung zu fördern.

Aufgrund der katalytischen Wirkung neuer Technologien ist zu erwarten, dass hybride Bedrohungen und hybride Kriegsführung zu langfristigen strategischen Herausforderungen werden. Daher ist es von entscheidender Bedeutung, ein umfassendes Verständnis ihrer technologischen Dimension zu entwickeln. Da sich die technologische Revolution mit einer noch nie dagewesenen Geschwindigkeit entfaltet, sind kontinuierliche Anstrengungen und ein flexibler und umfassender Ansatz aller relevanten Akteure in einem Gesamtkonzept von Regierung, Staat und Gesellschaft erforderlich. Aus diesem Grund ist es für die EU, die NATO und die Mitgliedstaaten mit allen relevanten Akteuren, Einrichtungen und Interessengruppen wichtig, ein solides Verständnis der neuen Technologien, ihrer künftigen Trends und ihres Störpotenzials für hybride Szenarien zu entwickeln, bevor sie – hoffentlich – mit den Auswirkungen der hybriden Kriegsführung konfrontiert werden. Das HYFUTEC-Projekt, das sich in dieser Monographie widerspiegelt, soll einen Beitrag in diesem Sinne leisten.

Wir danken allen, die zu diesem Projekt beigetragen, seine Veranstaltungen unterstützt, Diskussionen und Gedankenaustausch ermöglicht und Beiträge und Fachwissen aus verschiedenen Bereichen geliefert haben. Besonderer Dank geht an Marina Dane, ie-editing.com, für die Bearbeitung des Manuskripts und die Unterstützung des Projekts sowie an Oberst Dr. Anton Dengg für die Unterstützung des Projekts als Fachexperte. Die in dieser Monographie zum Ausdruck gebrachten Ansichten, Gedanken und Meinungen sind alleiniges Eigentum der Autoren.

Dr. Johann Schmid
Direktor COI Strategie und Verteidigung (COI S&D),
European Centre of Excellence for Countering
Hybrid Threats (Hybrid CoE)
Helsinki, Finnland

Ralph Thiele
Geschäftsführender Direktor, StratByrd Consulting
Andernach, Deutschland

Zusammenfassung

In einer Zeit des globalen Wettbewerbs um Sicherheitsarchitekturen, Handels- und Investitionsregime und die Vorreiterrolle bei neuen Technologien gewinnen hybride Szenarien *unterhalb der Schwelle zum Krieg* immer mehr an Bedeutung. Die hybride Kriegsführung hat sich zu einem effektiven, scheinbar *risikoarmen Machtinstrument* entwickelt. Russland, China, der Iran und weitere staatliche und nichtstaatliche Akteure nutzen geschickt kostengünstige, kommerziell verfügbare, neue Technologien, um ihre eigenen Ambitionen und Machtziele voranzutreiben. Sie integrieren den zivilen und militärischen Wettbewerb auf allen Ebenen, einschließlich der Entwicklung ihres internationalen Handels, ihrer Investitionen, ihrer nationalen Technologiebasis und ihrer politischen und diplomatischen Aktivitäten. Nicht nur Großmächte sind herausgefordert, sondern einfach alle – größere und kleinere Staaten, Unternehmen, Gesellschaften und einfache Bürger. Frieden und Freiheit, eine auf Regeln basierende Ordnung und Demokratie, Wohlstand und eine selbstbestimmte Lebensweise stehen auf dem Spiel.

China und Russland haben ihren technologischen Rückstand in den letzten zwei Jahrzehnten verringert, indem sie in einigen Fällen schneller und effektiver als ihre westlichen Konkurrenten auf kommerziell verfügbare Technologien zurückgegriffen und ihre eigenen Innovationen in den Streitkräften beschleunigt haben. Vor allem China hat *beeindruckende Schritte in Richtung technologischer Führerschaft* unternommen. Es hat bereits einen Vorsprung bei KI und 5G und ist auf dem besten Weg, andere Technologien wie Mikroelektronik und Quantencomputing zu dominieren. Gemeinsam mit Russland spielt es ein raffiniertes Spiel, indem es technologische Innovation als Mittel zur Durchsetzung eigener Ziele nutzt, ohne auf Krieg zurückgreifen zu müssen.

Die Vielzahl der sich abzeichnenden dynamischen und vor allem digitalen technologischen Entwicklungen deutet darauf hin, dass *das Portfolio hybrider Bedrohungen rasch wachsen wird*. Im Rahmen des Horizontscannings von Future & Technology wurden 19 technologische Trends identifiziert, die für die Entwicklung hybrider Szenarien sowie für die Möglichkeiten zur Bekämpfung hybrider Gegner relevant sind, nämlich: künstliche Intelligenz, 5G, autonome Systeme, Biotechnologie, Cloud Computing, Kommunikation, Cyber- und elektronische Kriegsführung, Distributed Ledger, gebündelte Energie, erweiterte Realität, Hyperschall, Internet der Dinge, additive Fertigung, Mikroelektronik, Nanomaterialien, Quantenwissenschaften, nukleare Modernisierung, Weltraum gestützte Technologien und allgegenwärtige Sensoren. Es ist wichtig zu verstehen, dass diese Technologien in ihrem sich gegenseitig verstärkenden *systemischen Zusammenspiel* besonders mächtig werden.

Aufkommende Technologien haben *das Schlachtfeld erweitert*, da sie hybride Akteure stärken, indem sie nicht nur neue Schwachstellen schaffen, sondern auch deren Ausnutzung erleichtern. Die *Rückkehr der Masse* auf das Schlachtfeld durch Drohnenschwärme und virtuelle Cyber-Roboter verdeutlicht die revolutionäre Dimension des bevorstehenden Wandels. Vor allem Technologien mit doppeltem/mehrfachem Verwendungszweck, Miniaturisierung und Automatisierung haben diese Entwicklung maßgeblich vorangetrieben. Viele dieser Technologien sind leicht zugänglich, erschwinglich, einfach zu handhaben, zu transportieren, zu verstecken und zu nutzen. Dies ermöglicht hybride Strategien, die Mehrdeutigkeiten ausnutzen und eine direkte Konfrontation vermeiden, z. B. durch die Nutzung sozialer Medien als Waffe, den Einsatz von Proxy-Akteuren oder die Störung des kognitiven Systems und des Vertrauenssystems des Feindes. Da diese Technologien auch nichtstaatlichen oder sogar individuellen Akteuren zur Verfügung stehen, kann diese Tendenz die Zahl der hybriden Akteure noch weiter erhöhen.

In Verbindung mit der Globalisierung wächst nicht nur *das Spektrum hybrider Akteure*, sondern auch die *Wirkung und Reichweite* ihrer Aktivitäten. Vor allem Angreifer werden von der Innovationsdynamik profitieren. Es ist zu erwarten, dass disruptive Technologien einer Vielzahl von Akteuren zusätzliche, leistungsfähige Optionen bieten werden, um im Rahmen hybrider Kampagnen Menschen, Vermögenswerte, kritische Infrastrukturen, komplexe Systeme und Prozesse virtuell und physisch anzugreifen, ohne dass die Gefahr einer Zuordnung oder unmittelbarer Vergeltungsmaßnahmen besteht. Diejenigen, die am besten in der Lage sind, technologische Entwicklungen zu antizipieren und auszunutzen, werden einen klaren Vorteil haben.

Wirksame Gegenmaßnahmen und Resilienz sind noch in der Findungsphase. Resilienz erfordert einen *gesamtgesellschaftlichen* Ansatz und ein umfassendes

Konzept, das permanent darauf abzielt, Schwachstellen und Bruchstellen zu verringern und den sozialen Zusammenhalt zu stärken. Dies ist umso wichtiger geworden, als der kommerzielle Sektor in Schlüsseltechnologien – mit wenigen Ausnahmen wie Nuklear-, Hyperschall- und elektronischer Kriegsführung – Technologiebereiche vorantreibt, die für Sicherheit und Verteidigung entscheidend sind, wie 5G, autonome Systeme, Biotechnologie, Cyber, Augmented Reality, künstliche Intelligenz, Lasertechnologien, Quantentechnologien, Robotik und Weltraumtechnologien. In den westlichen Demokratien ist der erforderliche Spinoff im Bereich der Verteidigungstechnologien noch nicht gut organisiert. Die diesbezügliche Beurteilung steht noch auf wackligen Beinen, was zu unzureichenden Einsatzkonzepten und Anforderungsdokumenten führt.

Sowohl am unteren (hybride Bedrohungen) als auch am oberen Ende des Konfliktspektrums (Hyperschall- und fortgeschrittene Kernwaffen) sind ernsthafte westliche *Fähigkeitslücken* entstanden. Sie öffnen die Tür für Nötigung und Erpressung. Gegner wie Russland, China oder der Iran werden absehbar politische, informationelle, kriminelle und infrastrukturelle Mittel sowie wirtschaftliche Einschüchterung und Manipulation einsetzen, um westliche Schwachstellen zu entdecken und auszunutzen.

Die Digitalisierung und die neuen Technologien sind jedoch nicht nur mit negativen Auswirkungen verbunden. Sie haben die Schaffung von Wohlstand auf der ganzen Welt vorangetrieben. Sie bieten auch wirksame Optionen, um hybride Herausforderungen besser zu erkennen, abzuwehren und zu bewältigen. So könnte KI beispielsweise dazu beitragen, das bereichsübergreifende Situationsbewusstsein in einer hybriden Konflikt-/Kriegsführungsumgebung zu verbessern. Sie ermöglicht im Großen und Ganzen die Modellierung eigener Schwachstellen oder hybrider Angriffsvektoren. Durch bahnbrechende und radikal verbesserte Technologien werden Netzwerke von Sensoren und Effektoren in die Lage versetzt, den Zyklus der Erkennung, Bewertung, Entscheidungsfindung und des Handelns von Zielen in mehreren Bereichen erheblich zu beschleunigen. Sie unterstützen auch den Einsatz von Serious Gaming, um Entscheidungsträger besser auf die Bewältigung neuer komplexer, hybrider *Systems-of-Systems-Herausforderungen* vorzubereiten.

Während wir davon ausgehen können, dass die hybride Kriegsführung zu einer langfristigen strategischen Herausforderung wird, stellt die Avantgarde der Innovation bereits die Weichen für ein postdigitales Zeitalter. Weder die Europäische Union noch die USA werden in der Lage sein, den technologischen Wettbewerb im Alleingang zu gewinnen. Die transatlantischen Partner sollten sich den technologischen Herausforderungen Russlands und dem technologischen Aufstieg Chinas gemeinsam stellen. Die EU, die NATO und ihre Mitgliedsstaaten wären gut

beraten, ihre strategischen Ambitionen nicht nur in wirtschaftlicher Stärke, sondern auch im technologischen Portfolio ihrer Streitkräfte widerzuspiegeln. Die Fähigkeit der NATO, der EU und der Mitgliedstaaten, Innovationen zu beschleunigen, wäre ein wesentlicher Bestandteil der Stärkung der Demokratie und der Gewährleistung von Wohlstand, Sicherheit und Verteidigung.

Inhaltsverzeichnis

Über die Autoren

Ralph D. Thiele, ist Präsident von EuroDefense, Deutschland, Vorsitzender der Politisch-Militärischen Gesellschaft, Deutschland und Geschäftsführer von Strat-Byrd Consulting, Deutschland.In seiner militärischen Laufbahn war Ralph Thiele in wichtigen nationalen und internationalen sicherheits- und militärpolitischen, planerischen und akademischen Funktionen tätig, u. a. im Planungsstab des Verteidigungsministers, im Kabinett des NATO Supreme Allied Commander Europe, als Stabschef an der NATO-Verteidigungsschule, als Kommandeur des Zentrums für Transformation der Bundeswehr und als Leiter der Lehre an der Führungsakademie der Bundeswehr. In seinen ehrenamtlichen und unternehmerischen Funktionen berät er zu den Themen Verteidigungsinnovation und Cyber in Zeiten der digitalen Transformation. Er hat zahlreiche Beratungen, Veröffentlichungen und Vorträge in Europa, Amerika und Asien gehalten.

Dr. Johann Schmid war von August 2018 bis September 2021 Direktor für COI-Strategie und Verteidigung am European Centre of Excellence for Countering Hybrid Threats in Helsinki (Finnland). In dieser Funktion initiierte er das Projekt „Hybrid Warfare Future and Technologies“ (HYFUTEC). Als Offizier der Bundeswehr war Dr. Schmid in einer Reihe verschiedener Verwendungen tätig, unter anderem in unterschiedlichen Funktionen/Missionen innerhalb der Kampftruppe des Heeres, in Einsätzen für die NATO sowie in der Wissenschaft. Von 2014 bis 2018 war er in der politischen Abteilung des deutschen Verteidigungsministeriums tätig. Seine wissenschaftliche Arbeit konzentriert sich auf die Theorie des Krieges mit einem besonderen Fokus auf hybride Kriegsführung.

Abkürzungen

5G	Technologiestandard der fünften Generation für zellulare Netzwerke
A2/AD	Anti-Access/Areal Denial
ACT	Allied Command Transformation
AIS	Automatic Identification System
AM	Additive Manufacturing
AR	Augmented Reality
ASAT	Anti-Satellite
AUV	Autonomous Underwater Vehicle
BMI	Brain-Machine Interface
BMS	Battlefield Management System
BRI	Belt and Road Initiative
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance
CBRN	Chemical, Biological, Radiological and Nuclear
CDE	Concept Development & Experimentation
CEO	Chief Executive Officer
C-IED	Counter Improvised Explosive Device
CIS	Combat Information Systems
CoG	Centre of Gravity
CoE	Centre of Excellence
COI	Community of Interest
COI S&D	Community of Interest Strategy & Defence

COMINT	Communications Intelligence
COPD	Comprehensive Operations Planning Directive
COTS	Commercial-Off-The-Shelf
COVID-19	Coronavirus Disease 2019
CSAR	Combat Search And Rescue
CSIS	Center for Strategic and International Studies
CSBA	(US) Center for Strategic and Budgetary Assessments
DARPA	Defense Advanced Research Projects Agency
DC/AC	Direct Current to Alternating Current
DEW	Directed-energy Weapons
DIME	Diplomatic, Informational, Military and Economic
DLT	Distributed Ledger Technology
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DOTMPLF	Doctrine, Organisation, Training, Materiel, Personnel, Leadership, Facilities,
EDA	European Defence Agency
ELINT	Electronic Intelligence
EMS	Electromagnetic Spectrum
EO	Electro-Optic
EOD	Explosive Ordnance Disposal
EU	European Union
EW	Electronic Warfare
FIN	Finland
FSB	Federalnaja sluschba besopasnosti Rossijskoi Federazii
GAN	Generative Adversarial Networks
GEO	Geostationary Orbit
GEOINT	Geospatial Intelligence
GIS	Geographic Information Systems
GNC	Guidance, Navigation and Control
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRU	Glawnoje Raswedywatelnoje Uprawlenije
GSM	Global System for Mobile Communications
HALE	High Altitude Long Endurance
HYFUTEC	Hybrid Warfare: Future & Technologies
ICT	Information and Communication Technology
IISS	International Institute for Strategic Studies
IoBT	Internet of Battle Things

INF	Intermediate-Range Nuclear Forces
EMP	Electromagnetic Pulse
FPA	Flat Panel Antenna
FuE	Forschung und Entwicklung
IO	Illuminator of Opportunities
IoBT	Internet of Battle Things
IoT	Internet of Things
IP	Intellectual Property
IR	Infrared
IRGC	Iranian Revolutionary Guard Corps
IRCM	Infrared Countermeasures
ISAR	Inverse Synthetic Aperture Radar
ISIS	Islamic State of Iraq and Syria
ISR	Intelligence, Surveillance, Reconnaissance
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
IT	Information Technology
JEDI	Joint Enterprise Defence Infrastructure
JRC	Joint Research Centre
JSTARS	*Joint Surveillance and Target Attack Radar System*
KI	Künstliche Intelligenz
KMU	Kleine Mittlständische Unternehmen
LED	*Light-Emitting Diode*
LEO	Low Earth Orbit
MASINT	Measurement and Signature Intelligence
MCM	Mine Countermeasures
MDA	Maritime Domain Awareness
MEO	Medium Earth Orbit
MMT	Man-Machine-Teaming
MR	Mixed Reality
M&S	Modelling & Simulation
NATO	North Atlantic Treaty Organization
NCW	Network Centric Warfare
NGO	Non-Governmental Organisation
NIST	*National Institute of Standards and Technology*
NSA	National Security Agency
NUAS	Nano Unmanned Aerial Systems
NWCC	NATO Warfighting Capstone Concept
OODA	Observe, Orient, Decide, Act (Beobachten, Orientieren, Entscheiden, Handeln)

OSINT	Open Source Intelligence
PGM	Precision-guided Munition
PMESII	Political, Military, Economic, Social, Infrastructure, Information
QC	Quantencomputing
QKD	Quantum Key Distribution
R&D	Research and Development
PaaS	Platform as a Service
PLA	People's Liberation Army
PLASSF	PLA Strategic Support Force
RAS	Robotic and Autonomous Systems
RF	Radio Frequency
RMA	Revolution in Military Affairs
RPAS	Remotely Piloted Aircraft Systems
SaaS	Software as a Service
SAR	Search-And-Rescue
SCADA	Supervisory Control and Data Acquisition
SIGINT	Signal Intelligence
SOCMINT	Social Media Intelligence
SPC	Single Photon Counting
STO NATO	Science & Technology Organization NATO
TTX	Table Top Exercise
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial Vehicle
US	United States
USD	United States Dollar
WMN	Wireless Mesh Networks
VR	Virtual Reality
XR	Extended Reality

Abbildungsverzeichnis