Kriegsführung der Zukunft

Informatisiert, entgrenzt, beschleunigt

FRANK SAUER
Geboren 1980 in Gelnhausen, Senior Research Fellow an der Universität der Bundeswehr München und Mitherausgeber des Podcasts „Sicherheitshalber“.

Die Zukunft hat die schlechte Angewohnheit, sich oftmals ganz anders zu entwickeln, als es das Verlängern von Trendlinien zuvor erwarten ließ. Statt Raketenrucksäcken, atombetriebenen Autos und Urlaub auf dem Mond brachte das 21. Jahrhundert das Internet, Smartphones und Twitter. Mit der vor diesem Hintergrund gebotenen Vorsicht identifiziert dieser Beitrag einige der charakterisierenden Elemente künftiger Kriegsführung.

Krieg, so das Clausewitz’sche Diktum, ist die Fortsetzung der Politik mit anderen Mitteln, also kein Selbstzweck, sondern ein dem Politischen nachgeordnetes (letztes) Mittel. Gemäß Artikel 2 Ziffer 4 der Charta der Vereinten Nationen ist Krieg zwischen Staaten ausschließlich zum Zwecke der Selbstverteidigung im Falle eines bewaffneten Angriffs zulässig. Realiter aber ist die organisierte und bewaffnete Gewaltausübung zwischen politischen Einheiten präsenter und auch vielgestaltiger. Vor dem Blick in die Zukunft dazu drei Beobachtungen aus der jüngeren Vergangenheit und Gegenwart.

Erstens: Krieg findet seit Ende des letzten Jahrhunderts vermehrt im Inneren von Staaten statt. Er wird dabei im Vergleich zu zwischenstaatlich

und mit regulären Streitkräften geführten Kriegen in der Regel militärisch weniger intensiv, zugleich aber mit größerem Blutzoll für die Zivilbevölkerung ausgetragen. *Zweitens* weist der Krieg der Gegenwart und jüngeren Vergangenheit zahlreiche Merkmale der Privatisierung und Ökonomisierung auf. Dafür spricht die rapide gestiegene Zahl privater Militärdienstleister oder auch das Phänomen der Warlords, für die Krieg ein Geschäftsmodell – also Clausewitz zum Trotz doch Selbstzweck – ist, nicht selten gespeist von politischem und religiösem Extremismus und Terrorismus. *Drittens* ist trotz der sogenannten neuen Kriege der klassische, zwischenstaatliche Krieg noch nicht Geschichte, wie die Invasionen im Irak, in Georgien oder auch der schwelende Konflikt in der Ostukraine und die Kampfhandlungen um Bergkarabach nahelegen. Aktuell gewinnt im Rahmen der Rivalität zwischen den USA und China sowie Russland das Paradigma des Großmachtkonflikts wieder an Bedeutung, inklusive des Rüstens für eine militärische Auseinandersetzung zwischen *near-peer competitors,* also zwischen militärisch (nahezu) ebenbürtigen Gegnern.

Drei direkt aufeinander bezogene Entwicklungen sind dabei für die künftige Kriegsführung besonders kennzeichnend: Informatisierung, Entgrenzung und Beschleunigung.

RINGEN UM EINFLUSS IM INFORMATIONSRAUM

Daten, so hört man häufig, seien das Öl des 21. Jahrhunderts. Die beliebte Analogie hinkt schon deshalb, weil Daten keine endliche fossile Ressource sind; sie macht jedoch auf einen wichtigen Zusammenhang aufmerksam. Daten sind für das digitale Zeitalter tatsächlich von zentraler Bedeutung. Staatliche und private Akteure wetteifern um die Möglichkeiten und Fähigkeiten zu ihrer Gewinnung sowie um die Kapazitäten, sie zu Informationen weiterzuverarbeiten. Die Transformation von Daten in Informationen verspricht ökonomische und, wenngleich ein deutlich schwierigeres Unterfangen, militärische Macht. Zivile Technologieunternehmen sind dabei die Innovationsmotoren.

In den USA sucht das Pentagon die Nähe zu Technologiefirmen im Silicon Valley. Die militärische Nutzung von Technologien der Künstlichen Intelligenz (KI) soll die globale militärische Vormachtstellung der USA absichern und ausbauen. Peking arbeitet ebenfalls an dieser sogenannten zivil-militärischen Integration. Die Früchte seiner rasanten kommerziellen Aufholjagd will China durch „Intelligentisierung“ seiner Kriegsführung auch in den Streitkräften nutzen.

Niedrigschwellig finden bereits – flankiert von Desinformation, Propaganda, Spionage und Handelskonflikten – eine (hybride) Konfliktaustragung und ein Ringen um Einfluss im Informationsraum statt. Dies reicht bis hin zu

Sabotage mittels Informationsoperationen, die in der physischen Welt Schaden anrichten. Die Zerstörung iranischer Urananreicherungszentrifugen mit der Schadsoftware Stuxnet war dafür der Vorbote.

ENTGRENZUNG ZIVILER UND MILITÄRISCHER SPHÄRE

Die militärische und geheimdienstliche Nutzung des Informationsraums wirft global bedeutsame Fragen zu Privatsphäre, Bürgerrechten und zur Zukunft eines freien und offenen Internet als öffentlichem Gut auf. Ein spezifischer Fallstrick mit Blick auf die Kriegsführung ist die drohende Verwischung der Grenze zwischen ziviler und militärischer Sphäre.

Ein Beispiel: Der Abwurf von Grafitbomben auf Umspannwerke zur Unterbrechung der Stromversorgung kann militärischen Zielen dienen, würde aber die Zivilbevölkerung überproportional in Mitleidenschaft ziehen – was öffentliche Kritik hervorruft, wie etwa im Rahmen des Balkankonflikts Ende der 1990er-Jahre tatsächlich geschehen, und auch völkerrechtliche Konsequenzen nach sich ziehen kann. Der gleiche Effekt lässt sich längst anonym – und zudem ohne Risiko für die eigenen Streitkräfte – per Informationsoperation bewerkstelligen, weil das sogenannte Attributionsproblem den Ursprung der Aktivität nicht verlässlich bestimmen lässt.

Die Konsequenzen sind dreierlei: *Erstens,* Abschreckung läuft ins Leere, weil unklar ist, an welche Adresse eine Vergeltungsdrohung zu richten wäre. *Zweitens,* Selbstverteidigung wird durch das Attributionsproblem zumindest erschwert, da sie aus völkerrechtlicher Sicht eigentlich unverzüglich nach dem Angriff gegen den Angreifer angewendet werden muss, um sie von Vergeltung zu unterscheiden. *Drittens,* Anonymität und die Bestreitbarkeit von Urheberschaft lassen die Versuchung wachsen, Kritische Infrastrukturen – wie etwa beim Beispiel der Stromversorgung – in militärische Zielkataloge aufzunehmen; mit entsprechenden Konsequenzen für die Zivilbevölkerung.

Das Vorbereiten von Informationsoperationen gegen Ziele eines künftigen potenziellen Kriegsgegners in Friedenszeiten entgrenzt nicht nur das Schlachtfeld – ein Phänomen, das sich in der exzessiven US-Drohnenkriegsführung auch physisch niedergeschlagen und ganze Teile des Globus zu latenten Kampfzonen gemacht hat. Es lässt auch die Grenze zwischen Kriegs- und Friedenszustand verschwimmen.

BESCHLEUNIGUNG UND DIE GEFAHR EINES „FLASH WAR“

Schon seit Jahrzehnten existieren automatische Verteidigungssysteme, die im Ernstfall viel schneller als ein Mensch Ziele auswählen und bekämpfen können. Automatisierung in Waffensystemen ist also weder neu noch per se

problematisch. Zur Abwehr von Beschuss bleibt sie unumstritten. In anderen militärischen Nutzungskontexten, die durch die zivil-militärische Integration von KI gegenwärtig erschlossen werden, birgt Waffensystemautonomie allerdings Risiken.

Zunehmende Autonomie oder Automatisierung von Waffensystemen bedeutet, dass mehr und mehr Funktionen nicht länger von Menschen, sondern vom Waffensystem selbst ausgeführt werden. Jede militärische Bekämpfung eines Ziels mit Waffengewalt durchläuft den gleichen Entscheidungszyklus. Im Rahmen dessen kann Autonomie einzelne Funktionen wie die Auffindung oder Verfolgung von Zielen beschleunigen, etwa mittels computergestützter Navigation oder Bilderkennung. Insbesondere aber die aus der Munitionsabwehr bereits bekannte Automatisierung der finalen Auswahl und Bekämpfung von Zielen ist militärisch bedeutsam, weil daraus ein entscheidender Geschwindigkeitsvorteil gegenüber von Menschen (fern)gesteuerten Waffensystemen erwächst. Folglich ist das aktuelle Ziel der Forschung und Entwicklung im Bereich konventioneller Hochtechnologie-Rüstung, alle erdenklichen fliegenden, fahrenden, schwimmenden oder tauchenden Waffensysteme künftig mit der Option zum autonomen Operieren und Bekämpfen von Zielen auszustatten.

Mit der Komplettierung des Entscheidungszyklus in Maschinengeschwindigkeit steigt die Gefahr nicht intendierter Eskalationen zwischen Streitkräften. Denn die Interaktionen zwischen softwaregesteuerten Waffensystemen sind nicht vorhersehbar. Von den Finanzmärkten sind durch den Hochfrequenzhandel die Risiken unvorhergesehener Interaktionsprozesse bekannt. Die dort vorkommenden *flash crashes* verursachen jedoch nur Kursabstürze und somit finanzielle Verluste; ungleich schwerwiegendere Konsequenzen hätte ein *flash war,* eine Kaskade aus blitzartig autonom initiierten Angriffen und Gegenangriffen, die in kürzester Zeit eine Eskalationsspirale in Gang setzen, ohne dass dem Menschen noch Zeit für einen korrigierenden Eingriff bliebe. In chinesischen Strategiedokumenten findet sich dafür der einprägsame Begriff der Schlachtfeldsingularität.

Eine andere Facette der beschleunigten Kriegsführung sind Hyperschallgleitflugkörper, also Trägersysteme, die mit Geschwindigkeiten von über Mach 5 fliegen. Russland, China und die USA treiben diese Entwicklung voran. Problematisch ist sie nicht, weil Hyperschallgeschwindigkeit bis zu Mach 20 etwas Neues wäre. Nach Wiedereintritt in die Atmosphäre sind die nuklearen Sprengköpfe schon seit Jahrzehnten genutzter ballistischer Raketen ebenso schnell. Problematisch ist vielmehr die Ambiguität der neuen Trägersysteme hinsichtlich ihres Sprengkopfs sowie ihres Ziels. Man weiß beim Anflug dieser neuen Waffenkategorie weder, ob es ein konventioneller oder nuklearer Angriff, noch, mangels ballistischer Flugbahn, was das Ziel desselben ist. Auch hier folgt aus Beschleunigung also Krisenstabilität.

EROSION INTERNATIONALER NORMEN

Die Informatisierung speist die Entgrenzung und die Beschleunigung der Kriegsführung. Die Folgen sind weitreichend: Der Unterschied zwischen Krieg und Frieden verwischt, an seine Stelle treten hybride Dauerkonflikte; in selbigen werden die Umrisslinien der kriegsvölkerrechtlichen Denkfigur des Kombattanten unscharf; das Schlachtfeld ist womöglich bald auch die eigene 5G-Infrastruktur, was den Unterschied zwischen zivilen und militärischen Zielen weiter aufweicht; selbst die ehemals rote Linie, die den Übertritt von der konventionellen zur nuklearen Kriegsführung markierte, verblasst im Lichte neuer konventioneller Hochtechnologie.

Mit anderen Worten: Mit der künftigen Kriegsführung droht die Erosion politischer, rechtlicher und ethischer Normen im internationalen System. Die Entwicklung von Waffensystemautonomie verdeutlicht diesen Dreischritt exemplarisch und mit großem Nachdruck: *Erstens* ist das mit Autonomie einhergehende sicherheitspolitische Eskalationsrisiko allgemein anerkannt, jedoch werden die Großmächte USA, Russland und China trotz ihrer Verantwortung, rüstungskontrollpolitische Leitplanken zu etablieren, nicht gerecht. *Zweitens* wäre der Einsatz autonomer Waffensysteme, so diese auch Menschenleben fordern, zumindest nach aktuellem Stand der Technik kaum mit dem Unterscheidungs- und Proportionalitätsgebot in Einklang zu bringen und liefe demzufolge Gefahr, das Kriegsvölkerrecht zu unterminieren. Hinzu kommt *drittens* die drohende Erosion der diesem Recht zugrunde liegenden humanitären Werte. Denn es verletzt die Würde des Menschen, Entscheidungen über Leben und Tod auf dem Schlachtfeld an Algorithmen zu delegieren, die Getöteten damit zu Objekten zu degradieren und zu entmenschlichen.

Die Europäische Union hat mit der Datenschutzgrundverordnung und dem Urteil des Europäischen Gerichtshofes zum Datenschutzabkommen *Privacy Shield* Entschlossenheit und den Willen zur Mitgestaltung eines wichtigen Aspekts der Informatisierung bewiesen. Der europäische Weg kann – muss! – die Alternative einerseits zu staatlichen Übergriffen nach dem Vorbild der Kommunistischen Partei Chinas und andererseits dem Überwachungskapitalismus des Silicon Valley werden. Diese Handlungsfähigkeit muss Europa auch auf anderen Feldern entwickeln. Denn mit Blick auf Entgrenzung und Beschleunigung ist es unsere Aufgabe, den Wandel aktiv und verantwortungsvoll, also im Einklang mit universellen Werten und Rechten, mitzugestalten und die Zukunft der Kriegsführung in Bahnen zu lenken, in denen das hart erkämpfte Kriegsvölkerrecht und der Respekt vor fundamentalen Normen wie der Menschenwürde bewahrt bleiben.