

## Potentiell autonome Waffensysteme



Seit Jahren warnen KI-Forscher\*innen, Völkerrechtler\*innen und Vertreter\*innen verschiedener UN-Organisationen vor der Entwicklung, dem Einsatz und der Weiterverbreitung sog. tödlicher autonomer Waffensysteme (Lethal Autonomous Weapon Systems, LAWS). Es handelt sich dabei um Waffensysteme, die ohne das Eingreifen von Menschen über den Einsatz tödlicher Gewalt entscheiden – umgangssprachlich werden sie auch als „Killerroboter“ bezeichnet.

Mittlerweile kommen u.a. in den Kriegen in der Ukraine und denen mit israelischer Beteiligung viele Waffen zum Einsatz, die über ein hohes Maß an Autonomie verfügen und zumindest potentiell als LAWS agieren und eingesetzt werden können. Ob und in welchem Umfang das bereits geschieht, ist jedoch unklar und umstritten – und wird es vermutlich auch noch bleiben. Denn die Frage, wo menschliche Kontrolle aufhört, ist ungeklärt. Viele Systeme – zum Beispiel Kamikazedrohnen – können eigenständig Ziele vorschlagen und im Zielflug verfolgen. Sie folgen unterschiedlichen Regelungen, falls die Funkverbindung abbricht, die durch ein einfaches Update oder das Bedienungspersonal geändert werden können. Außerdem kommen immer mehr unbemannte Systeme in sog. Schwärmen zum Einsatz, die als ganzes von einzelnen Menschen gesteuert werden oder gar autonom zuvor definierte Aufgaben erfüllen, etwa ein bestimmtes Gebiet zu überwachen. Auch bei Systemen zur sog. „Entscheidungsunterstützung“, die z.B. Ziele vorschlagen (die dann auch mit konventionellen Waffen angegriffen werden können), handelt es sich streng genommen nicht um tödliche autonome Waffensysteme – obwohl sie z.B. in Gaza Berichten zufolge massenhaft und nahezu ohne menschliche Kontrolle zur Bombardierung ziviler Ziele beigetragen haben. Wir schlagen deshalb vor, statt LAWS in einem engeren Sinne v.a. „Potentiell autonome Waffensysteme“ zu untersuchen und zu problematisieren und versuchen, das mit diesem Factsheet zu umreißen.

## Appell von 2016

„Autonome Waffen wählen und bekämpfen Ziele ohne menschliches Eingreifen. Dazu gehören z.B. bewaffnete Quadrocopter, die nach Menschen suchen und sie eliminieren, wenn sie bestimmte vordefinierte Kriterien erfüllen. [...] Technologien mit künstlicher Intelligenz (KI) sind an einem Punkt angelangt, an dem die Entwicklung solcher Systeme – zumindest praktisch, wenn auch nicht legal – innerhalb von Jahren und nicht Jahrzehnten möglich ist. [...]

Wenn eine der militärischen Großmächte die Entwicklung von KI-Waffen vorantreibt, ist ein globaler Rüstungswettlauf praktisch unvermeidlich. Und der Endpunkt dieser technologischen Reise ist offensichtlich: Autonome Waffen werden die Kalaschnikows von morgen werden. Anders als Atomwaffen benötigen sie keine kostspieligen und schwer zu beschaffenden Ausgangsstoffe, also werden sie allgegenwärtig und für alle maßgeblichen Militärmächte günstig zu produzierende Massenware werden. [...]

Einen militärischen Wettlauf um KI-Waffen zu beginnen ist eine schlechte Idee und sollte durch ein Verbot autonomer Angriffswaffen, die nicht von Menschen gesteuert werden, unterbunden werden.“

Autonomous Weapons Open Letter: AI & Robotics Researchers, Februar 2016

## Kamikazedrohnen für die Bundeswehr

Anfang April 2025 teilte das Bundesverteidigungsministerium mit, Kamikazedrohnen (Fachausdruck: Loitering Munition) für die Bundeswehr anschaffen zu wollen. Dabei handelt es sich um unbemannte Luftfahrzeuge, die mit einem Sprengsatz ausgestattet sind, mit dem sie sich in ein Ziel stürzen können. Davor können sie einige Zeit über dem Zielgebiet kreisen und potentielle Ziele aufklären und verfolgen. Im Februar 2026 beschlossen der Haushalts- und Verteidigungsausschuss die Anschaffung von zunächst je 2.000 bis 5.000 solcher Drohnen bei zwei deutschen Startups (Helsing und Stark Defence), die zuvor bereits umfangreich die ukrainische Armee beliefert und große Produktionskapazitäten aufgebaut hatten. Später kam ein weiterer Auftrag in ähnlichem Umfang an Rheinmetall hinzu. Die Drohnen sollen zunächst vor allem durch die deutsche Panzerbrigade in Litauen eingesetzt und getestet und dabei auch laufend weiterentwickelt werden. Für die erste Tranche von zunächst einigen tausend Stück zahlt die Regierung je knapp 300 Mio. an die betreffenden Unternehmen, das Gesamtvolumen der Rahmenverträge umfasst jedoch fast 7 Mrd. Euro.

Die technischen Spezifikationen der deutschen Kamikazedrohnen sind geheim, ihre Reichweite wird mit etwa 100km angegeben. Die Hersteller betonen gerne die hohe Autonomiefähigkeiten und dass die Drohnen auch im Stande wären, ihre Mission nach Abbruch der Funkverbindung – also ohne menschliche Kontrolle – zu beenden. Ziemlich sicher können diese Drohnen auch ohne menschliche Aufsicht im Einsatzgebiet manövrieren, mögliche Ziele identifizieren und verfolgen. Diese Ziele dann auch autonom anzugreifen, ist technisch sicher möglich, aber politisch wie militärisch vermutlich (noch) nicht gewollt.

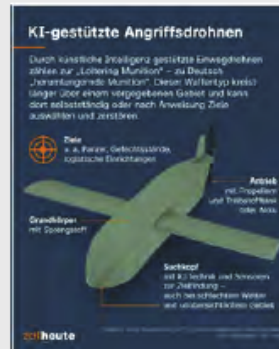
Insbesondere in der Ukraine kommen solche (taktischen) Drohnen schon massenhaft an der Front zum Einsatz, die sich auch dadurch eher in eine „Todeszone“ verwandelt hat. Russland, die Ukraine und der Iran nutzen auch noch andere Arten von Kamikazedrohnen für strategische Angriffe im Hinterland. Diese haben meist eine deutlich größere Sprengladung und Reichweite und werden über hunderte von Kilometern – ähnlich einem Marschflugkörper – in zuvor definierte Ziele geflogen. Durch Elektronische Kampfführung wie Jamming und Hacking können sie auch entführt und abgelenkt werden, sodass diese Drohnen manchmal auch in Drittstaaten auftauchen oder einschlagen.

## Drohnenwall und Schwärme

Seit 2024 werden in Deutschland und Europa Produktionskapazitäten aufgebaut, um zehntausende Drohnen kleiner und mittlerer Größe monatlich zu bauen. Die Unternehmen – viele davon neue Startups – und die Investor\*innen haben daraufhin, Anfang 2025, die Idee eines Drohnenwalls, bestehend aus zehntausenden Aufklärungs- und Kamikazedrohnen an der NATO Ostflanke propagiert. Später wurde der Drohnenwall eher als eine Abwehr gegen Drohnen diskutiert und Kommissionspräsidentin Ursula von der Leyen verkündete feierlich „der Drohnenwall wird kommen“.

Es war klar, dass eine solch große Menge an unbemannten Systemen nicht einzeln von Menschen gesteuert werden sollen. Verschiedene Unternehmen – darunter Helsing – boten Software zu Schwarmsteuerung der Drohnen an. Auch die Auswertung der massenhaft anfallenden Sensordaten müsste eine KI übernehmen, die dann vermutlich auch Handlungsempfehlungen ans Personal (s. Entscheidungsunterstützung) geben oder womöglich selbst Gegenmaßnahmen einleiten könnte.

Die Unternehmen behaupteten, so ein Drohnenwall wäre innerhalb eines Jahres realisierbar. Das war nicht realistisch angesichts der notwendigen Infrastruktur (Depots, Kommunikationssysteme, Kontroll-



„Dieser Waffentyp kreist länger über einem vorgegebenen Gebiet und kann dort selbstständig oder nach Anweisung Ziele auswählen und zerstören“ - Ganz beiläufig wird in dieser ZDF-Infografik die Frage offen gelassen, ob es sich bei den für die Bundeswehr beschafften Kamikaze-

drohnen um tödliche autonome Waffensysteme (LAWS) handelt. Auf die Bemühungen der UN, solche Waffen zu ächten, und die Warnungen bedeutender Wissenschaftler vor solchen Waffen wurde auch im dazugehörigen Beitrag „Bundeswehr rüstet Drohnenabwehr auf“ nicht eingegangen. Abbildung: ZDF-Infografik ([link](#))



Stark Virtus



Helsing HX-2



Rheinmetall FV-014

zentren), Verträgen zur Wartung und der hierfür notwendigen Logistik, Ausbildung des Personals, Entwicklung einer Einsatz-Doktrin usw. Vor allem die Realisierbarkeit einer halbwegs sicheren Schwarmsteuerung für so viele Systeme wurde von Fachleuten angezweifelt.

Trotzdem werden vergleichbare Projekte – in realistischerem Umfang und Zeitrahmen – durchaus bereits verfolgt. Eines davon ist die „Eastern Flank Deterrence Line“ EFDL, welche die NATO Stück für Stück umsetzt.

Am Konzept des Drohnenwalls gab es auch Kritik von Menschen, die grundsätzlich durchaus für eine massive Aufrüstung gegen Russland und auch keine Bedenken gegen den Einsatz von Drohnen mit hohem Grad an Autonomie haben. Unter dem Titel „Stoppt den Hype um Drohnen“ erinnerten Claudia Major und Christian Mölling daran: „Die Ukraine kommt mit den Drohnen dem Sieg (leider) nicht näher“. Die NATO setze hingegen auf „überlegene Feuerkraft und hohe Mobilität der Truppen“ mit der gegnerische Ziele schon weit jenseits des eigenen Territoriums bekämpft werden könnten. Sie stellen infrage, ob „westliche Gesellschaften das geringe Tempo und die starke Abnutzung eines Drohnenkriegs mit täglichen Opfern in Schützengräben“ durchhalten würden.

Tatsächlich haben die aktuell massenweise produzierten Kamikazedrohnen nur eine maximale Reichweite von etwa 100km. Das bedeutet, das Wartungs- und Bedienpersonal würde innerhalb der Reichweite gegnerischer Waffensysteme operieren. Was das bedeutet, kann man in der „Todeszone“ entlang der ukrainischen Front sehen. Hier sind Vorstöße nur in kleinsten Einheiten – durch drei, zwei oder auch nur einzelne Soldaten – möglich und gleichen trotzdem oft Himmelfahrtskommandos. Selbst im Erfolgsfall müssen die Überlebenden dann oft wochen- oder monatelang in Erdlöchern und anderen Verstecken ausharren ohne entdeckt zu werden, versorgt wiederum v.a. durch unbemannte Systeme.

## „Entscheidungsunterstützung“ und „Battle Management“

KI kommt in Kriegen und militärischen Übungen auf verschiedenen Ebenen auch in Form von sog. „Entscheidungsunterstützung“ zum Einsatz. So wirbt z.B. die Vected GmbH aus Fürth für ihre Zielfernrohre auf Infrarot-Basis (Wärmebild), in denen bereits KI integriert ist und im Bild Personen markiert und ein Wert angegeben wird, der die Wahrscheinlichkeit angibt, mit der es sich bei der jeweiligen Person um eine Bedrohung handelt.

Ähnliche Systeme kommen mittlerweile zunehmend auch in größeren Waffensystemen, wie etwa Schützenpanzern zum Einsatz, die ihre Bordwaffe bereits selbstständig auf entsprechende Ziele ausrichten können und dann nur noch auf den Feuerbefehl warten. Auch in Kampfflugzeugen und Satelliten kommen solche KI-Systeme zur „Entscheidungsunterstützung“ bereits zum Einsatz oder werden gerade nachgerüstet. Typischerweise operieren sie mit Wahrscheinlichkeitswerten. Einen Richtwert, ab welchem Schwellenwert ein Ziel beschossen wird, können dann zum Beispiel die von der militärischen Führung vorgegebenen Einsatzregeln (Rules of Engagement) liefern. Trotzdem soll theoretisch ein Mensch über den Einsatz von Waffengewalt entscheiden und dabei den Gesamtkontext – z.B. die Wahrscheinlichkeit ziviler Opfer und Schäden an nahegelegenen Infrastrukturen – berücksichtigen.

In der Praxis kommen Systeme zur „Entscheidungsunterstützung“ zunehmend nicht nur in einzelnen Waffensystemen und Plattformen zum Einsatz, sondern auf einer übergeordneten Ebene, in der verschiedene Waffen und Sensoren – von den einzelnen Soldat\*innen über eine Vielzahl bewaffneter und unbewaffneter Drohnen bis hin zu Panzern, Kampfflugzeugen, Schiffen und Satelliten – miteinander über ein „Battle Management System“ vernetzt



Einer der lautesten Fürsprecher des Drohnenwalls war Gundbert Scherf, Gründer und CEO des Drohnenstartups Helsing, der zuvor im Kontext der sog. „Berateraffäre“ unter Von der Leyen aus der Unternehmensberatung McKinsey ins BMVg geholt wurde.

## EFDL – Eastern Flank Deterrence Line

„Der Grundgedanke ist, ein komplexes, mehrschichtiges Verteidigungssystem entlang der Grenze zu Russland und Belarus aufzubauen und zur Verteidigung nicht nur konventionelle Truppen einzusetzen, sondern durch Hindernisse und den Einsatz von Technik eine roboterisierte oder automatisierte Zone im grenznahen Bereich zum Gegner zu schaffen, die dieser dann erst einmal überwinden muss. [...] Es geht um die Installation eines Systems von Sensoren und Effektoren, die miteinander in einem großen, digitalen Netzwerk verbunden sind, zur Einrichtung einer automatisierten Zone. [...] Es soll ein cloudbasiertes Netzwerk aufgebaut werden. KI-gestützte Systeme – inklusive generativer Modelle und maschinellem Lernen – verdichten die Aufklärungslage in Echtzeit und leiten sie unmittelbar an die eingesetzten Kräfte weiter. Dieses cloudbasierte Gefechtsnetz bildet das Nervensystem der Eastern Flank Deterrence Line und macht Mensch und Maschine zu einem eng abgestimmten Team. [...] Ich denke, dass man [...] versuchen wird, einvernehmliche Lösungen mit lokalen Gemeinschaften zu finden. Viele der Einrichtungen und Hindernisse werden erst im Falle eines bevorstehenden Einsatzes aktiviert und eingesetzt werden. Dies minimiert die dauerhafte Beeinträchtigung des zivilen Lebens. Es wird keine Massenumsiedlung geben.“

Bundeswehr-Brigadegeneral Thomas Lowin gegenüber der Welt am Sonntag vom 26.1.2026 über die im Aufbau befindliche EFDL.

## Aktiv werden!

Neben führenden Wissenschaftler\*innen haben sich u.a. der **UN-Generalsekretär António Guterres** und der **Papst Leo XIV.** für ein Verbot autonomer Waffensysteme ausgesprochen und vor den Gefahren militarisierter KI gewarnt.

Weltweit sind verschiedene Zivilgesellschaftliche Gruppen zu dem Thema aktiv, darunter das „**Future of Life“-Institut** und das **International Committee for Robot Arms Control (ICRAC)**. Die **Campaign to Stop Killer Robots** unterstützt Bemühungen zur Regulierung von LAWS auf Ebene der UN, ihr deutscher Ableger stellt auch deutschsprachiges Kampagnenmaterial zur Verfügung.

Verschiedene Gruppen der Friedensbewegung sind darüber hinaus zum Thema aktiv, darunter die **Deutsche Friedensgesellschaft – Vereinigte KriegsdienstgegnerInnen (DFG-VK)**, die **IPPNW** (Internationale Ärzt\*innen für die Verhütung des Atomkrieges, Ärzt\*innen in sozialer Verantwortung) und auch die **IMI**. Das **Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIFI)** hat sich u.a. mit seiner Kam-

## Die Praxis im Krieg

„Den ersten Roboter, den wir an der Front eingesetzt haben, haben wir verloren. [...] Weil wir ihn so gebaut haben, dass er den deutschen Sicherheitsvorschriften genügt hat. Dazu gehört ein Notausknopf, mit dem man das System sofort stoppen kann, wenn es etwas macht, was es nicht machen soll. Die Ukrainer haben uns gefragt: Was soll der Knopf? Das Letzte, was wir wollen, sagten sie, ist, dass jemand das System ausmachen kann. [...] Unser Learning daraus: Wir vergessen jetzt mal diese deutsche und die europäische Regulatorik, die Arbeitsplatz- und Verkehrssicherheit et cetera et cetera, die sogar Blinker für den Leopard 2 verlangt, und schärfen das System so, dass man damit in einem realen Krieg bestehen kann. [...] Der Bundeswehr haben wir gesagt, wir haben zwei Versionen des Systems. Eine für euch und eine für den Krieg. Und, by the way: Die für die Bundeswehr ist wegen der ausufernden Regulatorik ein Drittel teurer.“

Marc Wietfeld, CEO der Drohnenfirma ARX Robotics, im Interview mit der Frankfurter Allgemeinen Sonntagszeitung (14.12.2025)

## United States of Palantir

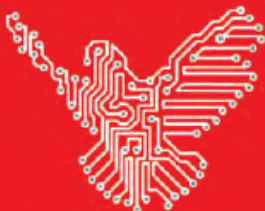
Anlässlich eines Mammut-Vertrages zwischen dem Pentagon und Palantir warnte die italienische Sozialwissenschaftlerin Francesca Bria im November 2025 unter dem Titel „United States of Palantir“ vor einer schleichenden Machtübernahme rechter Tech-Eliten durch „das systematische Outsourcing staatlicher Souveränität an US-Technologiefirmen“:

„Der Palantir-Deal bedeutet, dass Entscheidungen über militärische Ziele und Truppenbewegungen oder die Auswertung geheimdienstlicher Informationen zunehmend durch Algorithmen erfolgen, die nicht von der militärischen Führung kontrolliert werden, sondern von der Leitung eines Unternehmens, die im Interesse der Aktionäre agiert. Das US-Militär hat also nicht einfach Software eingekauft, vielmehr hat es seine operative Eigenständigkeit an eine Plattform abgetreten, ohne die es nicht mehr handlungsfähig ist.“

pagne „Cyberpeace“ zu diesen Fragen positioniert und man könnte darauf hinarbeiten, das auch der **Chaos Computer Club (CCC)** sich wieder verstärkt diesem Thema widmet.

In verschiedenen Städten (z.B. Nürnberg, Hannover, Berlin) existieren **Initiativen gegen Rüstungsmessen**, auf denen potentiell autonome Waffensysteme beworben werden oder gegen Forschungscluster und Industrieparks, in denen sie entwickelt werden. Bundesweit kämpfen Studierende und Wissenschaftler\*innen zusammen mit der lokalen Friedensbewegung für **Zivilklauseln** und setzen sich kritisch mit **Forschungsprojekten zu KI und autonomen Waffensystemen** auseinander.

Wer aktiv werden will, kann sich gerne an die Informationsstelle Militarisation wenden. Gerne vermitteln wir auch Referent\*innen zum Thema für **Vortragsveranstaltungen** oder **Filmvorführungen**.



KI-unterstützte Echtzeitauswertung von Wärmebildkameras, Bild: VECTED GmbH

sind. Dadurch fallen in jedem Augenblick eine riesige Menge an Daten an, die mithilfe von KI verarbeitet und zu einem Echtzeit-Lagebild verdichtet werden sollen. Ein Teil dieser Systeme ist eine Software, die Sensoren und „Schützen“ (Sensor-to-Shooter, S2S) miteinander vernetzt und dann den einzelnen Soldat\*innen, Drohnen, Waffentürmen etc. auf der Grundlage von Parametern wie Sichtlinie, Munitionsstatus etc. Ziele „vorschlägt“ und die entsprechenden Koordinaten liefert. Das US-Unternehmen Palantir behauptet z.B. mit seiner Software zwischenzeitlich den Großteil der Ziele für ukrainische Artillerieangriffe definiert zu haben.

Die israelischen Streitkräfte setzten im Rahmen ihrer Angriffe auf Gaza in großem Maßstab KI-Systeme ein, um mögliche Ziele zu bestimmen. Eines dieser Systeme hieß „Lavender“ und ordnete nahezu jeder dort lebenden Person auf der Grundlage von Massenüberwachung, Metadaten, Drohnenüberwachung etc. einen individuellen Wert zu, der die Wahrscheinlichkeit angab, mit der es sich um „Kämpfer der Hamas“ oder anderer bewaffneter Organisationen handle. So wurden in kürzester Zeit 37.000 Ziele „produziert“, die quasi per Copy & Paste in weitere Systeme übertragen werden konnten. Die Zeit zur Überprüfung der einzelnen Ziele durch Menschen habe dann nur noch 20 bis 60 Sekunden betragen. Ein anderes KI-gestütztes System mit dem zynischen Namen „Where’s Daddy?“ schlug an, wenn entsprechende Personen die mit ihnen verknüpfte Wohnung aufsuchten – wo sie vorzugsweise angegriffen und damit oft ihre ganze Familie getötet wurde. Die konkreten Angriffe erfolgten dann aber überwiegend durch bemannte Kampfflugzeuge oder Drohnen, die von Menschen gesteuert wurden.

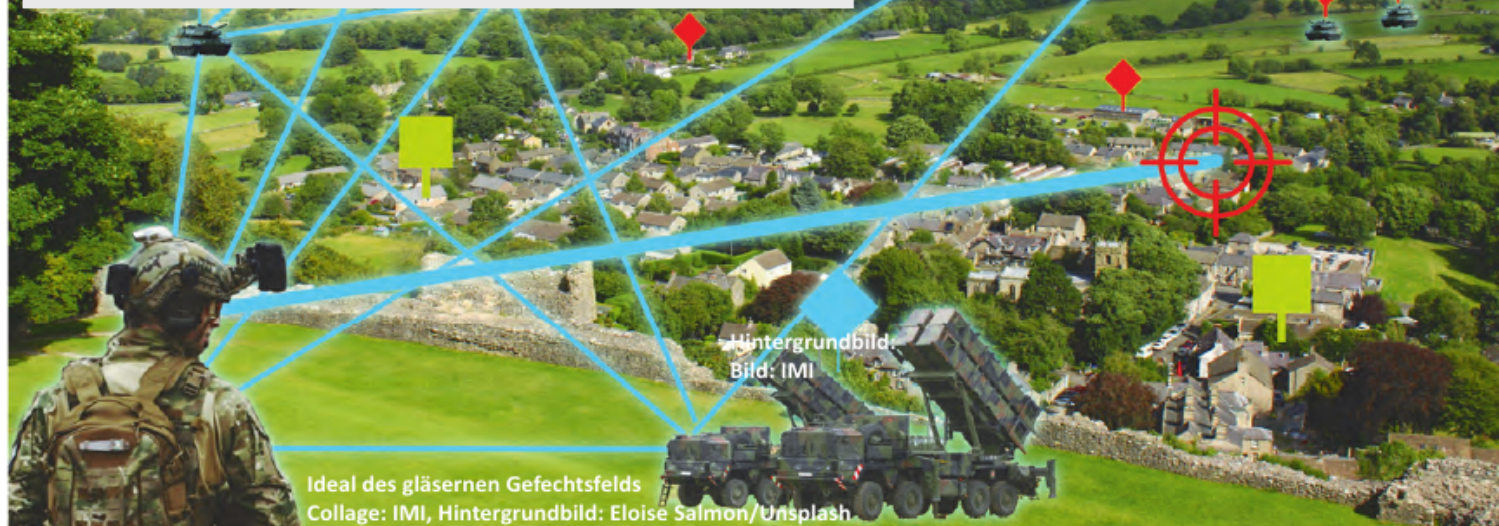
Bei den gemeinsamen Angriffen der USA und Israels auf den Iran haben die USA nach Angaben Cameron Stanleys, Verantwortlicher für Künstliche Intelligenz im Pentagon, mithilfe von KI in den ersten 96 Stunden des Kriegs 2.000 Ziele bombardiert. Dabei hat offenbar eine speziell für das Kriegsministerium lizenzierte Version des Chatbots „Grok“ von xAI (Elon Musk) als Schnittstelle zum System „Maven Smart System“ von Palantir (Peter Thiel) gedient. In Werbevideos von Palantir werden Systeme vorgestellt, die Militärs über einen Chatbot eigenständig taktische Vorschläge zur Planung und Durchführung von Operationen unterbreiten – und diese angeblich auf entsprechende Bestätigung hin auch in die Wege leiten können.

Formal gesehen handelt es sich bei solchen Systemen zur „Entscheidungsunterstützung“ und dem „Battal Management“ nicht um autonome Waffensysteme. Da die Integration von autonomen Aufklärungs- und Analysesystemen mit „Wirkmitteln“ jedoch gerade rasant voranschreitet, sollten sie zumindest als potentiell autonome (Groß-)Waffensysteme betrachtet werden – im Grunde gar als KI-basierte Streitkräfte mit schwindendem Maß menschlicher Kontrolle. Am Beispiel des Iran hat die IMI die These eines bereits stattfindenden „strategischen Kontrollverlustes“ durch den Einsatz von KI in den Raum gestellt, weil diese – entkoppelt vom tatsächlichen militärischen Nutzen – nahezu unbegrenzt neue Ziele produzieren kann: „Dass sich der Fokus militärischen Handelns vom eigentlichen politischen Ziel zunehmend auf eine fortsetzbare und fortgesetzte Zerstörung als Selbstzweck verlagert.“

## Positiver Effekt von Krieg

„So bitter dieser Krieg ist, hat er aber einen positiven Effekt: Wir sehen eine militärtechnologische Entwicklung, die so rapide vorangeht, wie wir sie ohne diesen Krieg nicht gehabt hätten. Darin liegt, noch einmal, bei aller Tragik dieses Krieges und bei allem furchtbaren Leid, die dieser Krieg über das Land und über die Menschen bringt, jetzt eben auch eine große Chance, die wir nutzen werden. Wir kommen technologisch in einer Geschwindigkeit voran, wie ich es nicht gedacht hätte, und das erlaubt uns auch eine sehr viel größere europäische Unabhängigkeit.“

Bundeskanzler Merz auf der Pressekonferenz nach dem Europäischen Rat auf Zypern am 24. April 2026



Die besonderen Chancen, die der Krieg für Start-ups im Bereich Drohnen und KI bietet, erläuterte Oberst Matthias Puschnig, Vize-Leiter des Sonderstabs Ukraine im BMVg, damit, dass dort der Einstieg nicht durch Bürokratie behindert würde: „... [I]n der Ukraine ist das alles egal, Hauptsache, man macht etwas, das sich von Westen nach Osten bewegt und dort Schaden erzeugt. Und wir denken jetzt an die deutschen Drohnen-Start-ups etwa, die gute Sachen haben, doch die konnten sie bisher nur dort verkaufen. Jetzt kommen sie aber mit dem Stempel 'battle proven' aus der Ukraine zurück und erhalten so auch hier auf dem Markt eine Chance.“ Dabei spielt das BMVg demnach eine aktive Rolle, so Puschnig weiter: „Tatsächlich mache ich jede Woche so 20 Anrufe und erkläre in Ruhe: Ja, es gibt Chancen in der Ukraine, fahre dahin, baue Geschäftskontakte auf, das ist kein Problem, die Ukraine ist sehr offen, sehr hilfsbereit. Sag, was du dort machen möchtest. Such dir einen Partner. Geht gemeinsam an die Streitkräfte ran, versuche dein Produkt zu platzieren.“ (Quelle Security.Table #426, 18. März 2026)

If technology development is to be iteratively improved through constant experimentation and trial and error, then war becomes reconfigured as an opportunity for experimentation. In this context, war becomes endless and everywhere, as it is only through experimentation in war that technological innovation, progress, or superiority can be sustained.

**Myth, Power, and Agency:** Rethinking Artificial Intelligence, Geopolitics and War.

## Experimentelle Kriegführung und Profit – Beispiel Ukraine

Bereits im Februar 2024 veröffentlichte Vera Bergengruen im Time Magazin einen vielbeachteten Beitrag unter dem Titel „How Tech Giants Turned Ukraine Into an AI War Lab“. Sie zitiert darin den damaligen ukrainischen Minister für digitale Transformation mit den Worten: „Unsere Mission besteht darin, die Ukraine in das größte Labor für Forschung und Entwicklung zu verwandeln“. Anfang 2026 wurde Fedorov Verteidigungsminister, nachdem er bereits zuvor Brave1, die ukrainische Abteilung für „Innovationen“ im Verteidigungssektor geleitet hatte. Wieder und wieder haben ukrainische Regierungsvertreter Rüstungsunternehmen eingeladen, ihre Waffen in der Ukraine zu testen, im Juli 2025 in Wiesbaden die offizielle „Test in Ukraine“-Initiative ausgerufen. Im Mittelpunkt stehen dabei Drohnen und andere unbemannte Systeme, die in der Ukraine quasi täglich in neuen Modellen und Variationen mit wachsendem Autonomiegrad zum Einsatz kommen. Bei Selenskyjs Besuch in Berlin im April 2026 und dem anschließenden Besuch von Pistorius in Kiew wurde offiziell eine Partnerschaft bei der Entwicklung von Drohnen – auch mit sehr großer Reichweite bis 1.500km – vereinbart.

Mittlerweile konnten sich dutzende deutsche Startups dadurch am Markt platzieren, dass sie – finanziert aus dem Bundeshaushalt – Drohnen zunächst an die Ukraine geliefert und dann als „gefechtserprobt“ auch in andere Länder exportieren konnten. Das gilt u.a. für die Unternehmen Helsing (geschätzter Marktwert Stand Juli 2026 18 Mrd. US\$) und Stark Defence (geschätzter Marktwert 3,5 Mrd. US\$, Investor u.a. Peter Thiel) die nun auch Kamikazedrohnen an die Bundeswehr liefern, sowie Quantum Systems (8 Mrd. US\$, auch hier ist Thiel beteiligt), Arx Robotix (ca 1 Mrd. US\$) und Donaustahl. Mithilfe von Risikokapital sind diese Unternehmen in kurzer Zeit so groß geworden, dass sie etablierte Firmen aufkaufen und internationale Joint Ventures, u.a. mit Unternehmen

aus den USA und der Ukraine, gründen konnten. Ihr explizites Ziel ist es, jeweils „zehntausende“ Drohnen pro Monat herzustellen und hierbei die Automobilindustrie einzubinden.

Zunächst konnten besonders im Großraum München viele Start-ups von Ukrainekrieg und Sondervermögen profitieren, haben dort sehr schnell neue Büro-Standorte und Produktionsstätten gebaut. München überholte dadurch 2024 London und Paris als die Städte in Europa, in den die meisten Risikokapitalinvestitionen in die Rüstungsindustrie fließen. Als Grund dafür wird oft auf die Rolle der Universitäten (TU München, Ludwigs-Maximilian-Universität, Bundeswehr-Universität) hingewiesen, die offen für Rüstungsforschung sind und Startup-Programme haben, sowie gelegentlich auf die dort der recht aktive „ukrainische Community“. Im Februar 2026 wurde vom BMVg in Erding bei München das „Innovationszentrum der Bundeswehr“ eröffnet – eine Art beständiger Rüstungsmesse mit Testgelände, auf der Vertreter\*innen der Bundeswehr und von Start-ups ständig präsent sind, Investor\*innen, weitere Industrievertreter\*innen und Angehöriger verschiedener Waffengattungen ein- und ausgehen. Mittlerweile wollen weitere Standorte, darunter Berlin und der Großraum Stuttgart das Münchner Modell kopieren.

Fest steht: internationales Risikokapital hat mit massiver Unterstützung der Bundesregierung in den letzten Jahren massiv in deutsche Rüstungs-Startups investiert, die Potentiell Autonome Waffensysteme entwickeln und massive Produktionskapazitäten aufgebaut haben. Diese Investitionen lohnen sich nur, wenn die gegenwärtige Aufrüstung anhält und die bestehenden Systeme kontinuierlich weiterentwickelt und ersetzt werden. Dabei wirkt die kontinuierliche, experimentelle Kriegführung in der Ukraine auch als Programm zur Umverteilung: Die Bundesregierung sichert durch Steuereinnahmen und die Aufnahme von Schulden die Profite deutscher Startups und des dahinterstehenden Risikokapitals. Auch in der Wissenschaft wird die Verflechtung staatlicher und privater Interessen im Kontext „experimenteller Kriegführung“ zunehmend thematisiert. So schreibt die Technikforscherin Marijn Hoijtink: „Wenn Technologieentwicklung durch kontinuierliches Experimentieren, Versuch und Irrtum verstetigt soll, wird Krieg als Chance für solches Experimentieren rekonfiguriert. In diesem Kontext wird Krieg endlos und allgegenwärtig, da nur durch ständiges Ausprobieren im Krieg technologische Innovation, Fortschritt und Überlegenheit gewährleistet werden kann“.

## Mit Steuergeldern an die Front

Im Juli 2026 gab das ukrainische Unternehmen Skyfall bekannt, dass ein europäischer Staat die Lieferung von 50.000 seiner Kamikazedrohnen vom Typ „Shrike“ an die Front finanziere. Ausgerüstet werden die Drohnen mit einer KI-Software des Unternehmens Auterion, welche den vollautonomen Zielanflug auch auf ausweichende Ziele sowie eine spätere Schwarmfähigkeit ermögliche. Auterion ist formal ein (zunächst 2017 in der Schweiz gegründetes) US-amerikanisches Unternehmen, das aber eine große Niederlassung in München hat, wo die betreffende Software entwickelt worden sein soll. Bei dem „europäischen Land“, das die Anschaffung im Wert von geschätzten 90 Mio. Euro finanziert, handelt es sich höchstwahrscheinlich um Deutschland.

## KI-Strategie des BMVg

Am 28. Juli 2026 hat das Bundesverteidigungsministerium seine KI-Strategie vorgestellt. Darin verabschiedet sich das BMVg vom Prinzip des „Human-in-the-loop“, wonach an jeder Entscheidung zum Einsatz einer Waffe ein Mensch beteiligt sein muss. Stattdessen wird das vage und flexible Konzept der „kontextabhängigen Kontrolle“ eingeführt, wonach eben der Kontext entscheiden sollte, wie viel Kontrolle noch beim Menschen liegen sollte. KI-Systeme sollen danach in großem Umfang bei der Bundeswehr eingeführt werden, von der Krisenfrüherkennung bis zur Überwachung der NATO-Ostflanke durch Sensornetzwerke und Schwärme unbemannter Systeme. Auch in intensiven Kampfhandlungen wie sog. Multi-Domain-Operationen sollen sie durch die Auswertung enorm großer Mengen von Daten in Echtzeit für „Informationsüberlegenheit“, „Führungsüberlegenheit“ und „Wirkungsüberlegenheit“ sorgen. Dass die menschliche Übersicht dabei auf der Strecke bleibt, ist anzunehmen.

## Autonome Cyberwaffen

„[...] Menschliche Hacker könnten durch lernfähige KI-Systeme ersetzt werden, die automatisch Schwachstellen finden. Dies kann genutzt werden, um Angriffsziele bei einem Gegner zu bestimmen, aber auch um in eigenen Systemen Lücken zu finden und zu schließen. KI-Methoden können helfen Cyberangriffe zu optimieren, das heißt besonders wichtige Infrastruktursysteme zu finden und einen günstigen Zeitpunkt zu bestimmen, um eine möglichst große Wirkung bei einem Angriff zu erzielen. [...] Dass sich LLMs [Large Language Models, Grundlage generativer KIs

wie ChatGPT] auch zur Durchführung von Cyberangriffen eignen, haben verschiedene Untersuchungen gezeigt. Bei entsprechenden Aufträgen können mögliche Angriffsziele gesucht und Angriffe geplant und ausgeführt werden. Nicht nur Menschen, sondern auch technische Systeme, also Bots können Aufgabenstellungen und Anfragen an LLMs stellen. Dies könnte natürlich auch Cyberangriffe betreffen, und damit können sich völlig autonome Cyberwaffen entwickeln, die noch nicht einmal extra gestartet werden müssen, denn diese Systeme sind ohnehin au-

tonom im Internet aktiv. [...] Auch bei vollautonomen Waffensystemen sind unvorhersehbare Interaktionen zwischen den automatischen Systemen möglich, die in eine Kettenreaktion von autonom geführten Angriffen und Gegenangriffen münden können. Hierbei kann in sehr kleinen Zeitintervallen eine Eskalationsspirale entstehen, die von Menschen nicht beherrscht werden kann.“

Karl Hans Bläsius: Künstliche Intelligenz und Krieg - Welche Risiken entstehen, wenn der Mensch die Kontrolle verliert?, Springer, Berlin 2026.