# Künstliche Intelligenz macht Tech-Firmen zu Rüstungsunternehmen. Damit werden sie zu militärischen Zielen

Ohne Daten lässt sich heute nicht mehr effizient Krieg führen. Das macht die Tech-Konzerne zu zentralen Akteuren. Die Risiken werden noch unterschätzt.

Lukas Mäder, NZZ 20.04.2026

An den Luftangriffen der USA auf Iran arbeiteten im Hintergrund amerikanische Tech-Firmen mit. Bei der Erkennung und der Auswahl von Zielen oder bei der Vorbereitung von Militäraktionen spielen KI-Modelle und Cloud-Dienstleistungen von Firmen wie Google, Amazon oder Microsoft eine wichtige Rolle. Daten sind die Grundlage der modernen Kriegsführung – und sie werden durch KI noch wichtiger.

Im Nahen Osten sind die Tech-Firmen zu einem militärischen Ziel geworden. Iran hat bereits am zweiten Tag des Kriegs drei Rechenzentren von Amazon in den Vereinigten Arabischen Emiraten und in Bahrain angegriffen. Inzwischen haben die iranischen Revolutionswächter eine Liste von 18 amerikanischen Tech-Firmen publiziert, die sie als legitime Ziele ansehen. Grund dafür sei, dass die Firmen mit dem amerikanischen Militär zusammenarbeiten.

Die Tech-Firmen befinden sich in einer neuen Rolle. Sie sind nicht mehr rein zivile Unternehmen. Der Einsatz von KI in der Kriegsführung macht sie in Teilen zu Rüstungsunternehmen. Das schafft neue Risiken, die noch zu wenig Beachtung finden.

## Daten werden zum Treibstoff der modernen Armee

Dass Daten entscheidend sind für die Kriegsführung, zeigt der Ukraine-Krieg. Die ukrainische Armee hatte bereits früh eine Plattform namens Delta geschaffen, auf der Daten praktisch in Echtzeit zusammenlaufen. Diese ermöglicht ein Bild der Lage, die Analyse und eine schnelle Reaktion. Die Fähigkeit, rasch zurückzuschlagen, brachte den Ukrainern zumindest zu Beginn des Kriegs einen Vorteil auf dem Gefechtsfeld.

Daten sind die Grundlage von KI-Anwendungen. Um sie verfügbar zu machen, braucht es eine entsprechende Infrastruktur. Dazu gehört die Vernetzung innerhalb der Truppe, sei es über Glasfaser- oder Kupferkabel, über Funk oder Satelliteninternet. Dass die Ukraine Zugriff auf das Satellitensystem Starlink hat, gilt als grosser Vorteil für deren Kriegsführung. Die Satellitenkommunikation lässt sich nur schwer stören und erlaubt einen grossen Datendurchsatz, um insbesondere Live-Aufnahmen von Drohnen zu übertragen.

Die Verarbeitung von Daten benötigt leistungsstarke Server oder ganze Rechenzentren. Diese Einrichtungen werden im Krieg zu relevanten militärischen Zielen. Als eine ukrainische Drohneneinheit im Februar Angriffe in den russisch besetzten Gebieten flog, zählte am gleichen Tag ein Rechenzentrum zu den Zielen, neben einem Militärflugplatz und einem Umspannwerk.

Der Datenfluss gehört in modernen Armeen heute zur Basisversorgung. Er ist nötig, um die Kampffähigkeit der Truppe sicherzustellen – genauso wie Nahrungsmittel, Treibstoff, Munition oder medizinische Hilfe. Die Datenmengen haben heute Ausmasse angenommen, die viele herkömmliche Kommunikationssysteme heillos überfordern.

# Künstliche Intelligenz macht Tech-Firmen zu Rüstungsunternehmen. Damit werden sie zu militärischen Zielen

Daten werden in Zukunft noch wichtiger für die Kriegsführung. Tech-Firmen, die das Militär mit KI-Programmen, Cloud-Lösungen und Kommunikationsdiensten versorgen, werden zu einem zentralen Akteur in Konflikten.

Armeen waren schon immer von den Rüstungsfirmen abhängig. Die Zusammenarbeit war eng. Die Waffenhersteller lieferten im Grundsatz jedoch abgeschlossene Systeme, über welche das Militär danach selbst verfügen konnte. Betrieb und Wartung waren, falls gewünscht, oft selbständig möglich, falls die Ersatzteile vorhanden waren. Mit dem Einzug von Software begann diese Trennlinie zunehmend zu verwischen.

KI in der Kriegsführung verändert die Kooperation mit den Zulieferern weiter. Bei der Datenverarbeitung sind die Verbindungen zwischen Militär und den privaten Zulieferfirmen nochmals deutlich enger. Dieselben Dienste werden sowohl zivil als auch militärisch genutzt. Diese zentrale Rolle der Tech-Firmen bringt Risiken, nicht nur für die Unternehmen selbst, sondern auch für die Armeen und die Gesellschaft.

Armeen werden von den Tech-Firmen abhängig. Im Herbst 2022 wollten die ukrainischen Streitkräfte mit Marinedrohnen einen Angriff auf die Krim durchführen und dafür eine Starlink-Verbindung einsetzen. Doch das Unternehmen schaltete die Satellitenkommunikation dafür nicht frei, der Angriff konnte nicht stattfinden. Für die US-Armee stellt sich dieses Problem weniger, weil viele wichtige KI- und Tech-Firmen amerikanisch sind. Das gibt der Politik die Möglichkeit, Druck auszuüben.

Sind zivile Dienste für die Kriegsführung entscheidend, werden sie zu legitimen Angriffszielen. Das vergrössert die Gefahr von Kollateralschäden. Weil die Vernetzung im technologischen Bereich gross ist, kann ein Angriff weit über die Konfliktparteien hinaus zu Ausfällen führen. Kritische Infrastrukturen von unbeteiligten Staaten können betroffen sein, die Wirtschaft leidet.

Dieses Szenario ist zu Beginn des Ukraine-Kriegs eingetreten. Damals griff Russland den privaten Satellitenkommunikationsdienst Viasat an, den die ukrainischen Sicherheitskräfte nutzten. In der Folge fielen Datenverbindungen von Windrädern in Deutschland oder Internetzugänge in Frankreich aus, die ebenfalls über Viasat funktionierten.

## Die US-Regierung will die Hoheit über ihre Tech-Firmen. Zivile Tech-Firmen werden zu engen Partnern.

Neue Risiken schafft die KI-Kriegsführung vor allem aber für die Tech-Firmen selbst. Sie versuchten lange, sich und ihre Dienste als politisch neutral zu präsentieren. Das war die Voraussetzung, um möglichst viele Märkte zu erschliessen und um Behörden oder Sicherheitsorgane als Kunden zu gewinnen.

Doch diese Erzählung bröckelt – wegen der veränderten geopolitischen Lage, aber auch wegen der neuen Rolle der Unternehmen selbst. Weil die Tech-Firmen zu Rüstungszulieferern werden, verlieren sie ihre Unabhängigkeit.

Spätestens im Fall eines bewaffneten Konflikts führt dies zu Problemen. Es drohen direkte militärische Angriffe auf die Infrastruktur der Firmen oder gezielte Cyberangriffe, um deren Dienste lahmzulegen. Die Firmen können wegen ihrer militärischen Kooperation in Kritik geraten: Ihre Reputation leidet, und Kunden wenden sich ab, was rasch wirtschaftliche Schäden verursacht.

# Künstliche Intelligenz macht Tech-Firmen zu Rüstungsunternehmen. Damit werden sie zu militärischen Zielen

Bei Google kam es 2017 zu interner Kritik, weil sich das Unternehmen am Projekt Maven des amerikanischen Verteidigungsdepartements beteiligte. Als die Proteste der Belegschaft zu stark wurden, zog sich Google aus dem KI-Projekt zurück. In die Lücke sprang das Unternehmen Palantir, welches wegen seiner engen Zusammenarbeit mit Armeen, Nachrichtendiensten und Polizeien konstant derartiger Kritik ausgesetzt ist.

Der Gaza-Krieg führte ab Ende 2023 zu Kritik an der Zusammenarbeit mit Israel. Microsoft löste im vergangenen Herbst Verträge mit dem israelischen Verteidigungsministerium auf, weil die Streitkräfte Cloud-Server in den Niederlanden zur systematischen Auswertung von Telekommunikationsdaten aus dem Gazastreifen verwendet hatten. Microsoft beharrte diesbezüglich auf seinen Nutzungsbestimmungen.

In den USA ist eine solche Positionierung inzwischen schwieriger geworden. Wer sich gegen die Wünsche der Regierung von Donald Trump stellt, geht ein enormes unternehmerisches Risiko ein. Das musste die KI-Firma Anthropic Ende Februar erfahren. Dem Unternehmen wurde zum Verhängnis, dass es seine KI-Modelle nicht für vollautonome Waffensysteme und nicht zur Massenüberwachung der einheimischen Bevölkerung zur Verfügung stellen wollte.

Als Reaktion darauf hat die amerikanische Regierung nicht nur den millionenschweren Vertrag mit Anthropic aufgelöst. Sie stuft das KI-Unternehmen zusätzlich als Risiko für die nationale Sicherheit ein – obwohl sie eben noch auf genau diese Technologie gesetzt hatte. Offensichtlich will die Regierung Anthropic für seine Haltung bestrafen. Der Firma drohen schwere finanzielle Schäden.

## KI macht Technologie politisch

Künstliche Intelligenz, Datenverarbeitung und Kommunikation sind heute strategisch wichtig. In Konflikten ist es für Staaten entscheidend, diese Prozesse möglichst weitgehend zu kontrollieren. Deshalb stehen jene Unternehmen unter politischem Einfluss, die diese Dienstleistungen anbieten. Technologie ist aus politischer Sicht nicht neutral.

Für die amerikanischen Tech-Konzerne entsteht dadurch ein erhebliches Risiko. Sie spüren seit dem Amtsantritt von Donald Trump ein grundsätzliches Misstrauen aus Europa. Ihre militärischen Verflechtungen lassen sie noch weniger als unabhängige Anbieter erscheinen.

Die Risiken dieser Entwicklung sind noch nicht überall erkannt. Für die Tech-Firmen werden die geopolitischen Entwicklungen zum unternehmerischen Risiko. Für Wirtschaft und Gesellschaft wird das aufkommende Primat der Politik zur Gefahr. Wer nicht in der Gunst der amerikanischen Regierung steht, kann sich immer weniger auf die US-Konzerne verlassen. KI im Krieg macht Technologie definitiv politisch.