https://strategic-culture.su/news/2026/03/28/war-without-borders-how-digital-revolution-has-transformed-21st-century-conflicts/

Krieg ohne Grenzen:
Wie die digitale Revolution die Konflikte des 21. Jahrhunderts verändert hat

In den letzten zwei Jahrzehnten hat die digitale Revolution eine zweite Ebene strategischer Infrastruktur geschaffen – unsichtbar, allgegenwärtig und tief in den globalen Volkswirtschaften verwurzelt.

28. März 2026 | Lorenzo Maria Pacini

Das unsichtbare Schlachtfeld

In traditionellen Kriegen konzentrierten die Armeen ihre Feuerkraft auf klar definierte und sichtbare strategische Ziele: Militärstützpunkte, Waffenfabriken, Flughäfen und Treibstoffdepots. Versorgungslinien ließen sich auf einer Karte nachverfolgen, Schlachtpläne mit relativer Sicherheit aufstellen und die Kampfkraft anhand von Zahlen, Feuerkraft und taktischen Manövern messen. Der Feind hatte ein Gesicht, eine Uniform und einen erkennbaren geografischen Standort.

All dies ist heute Teil einer Kriegslogik, die zunehmend an Bedeutung verliert. In den letzten zwei Jahrzehnten hat die digitale Revolution eine zweite Ebene strategischer Infrastruktur geschaffen – unsichtbar, allgegenwärtig und tief in den globalen Volkswirtschaften verwurzelt –, die still und leise die Art und Weise verändert hat, wie Macht ausgeübt und Krieg geführt wird. Die digitale Infrastruktur hat sich vom Rand des Konflikts in dessen operativen Kern verlagert.

Informationsbeschaffung, Drohnenkoordination und Entscheidungsfindung auf dem Schlachtfeld: Alles hängt zunehmend von Cloud-Systemen und Plattformen für künstliche Intelligenz ab. Die Architektur zeitgenössischer Konflikte stützt sich ebenso sehr auf von privaten Unternehmen verwaltete Netzwerke wie auf konventionelle militärische Hardware.

Diese sich wandelnde Realität hat tiefgreifende geopolitische Auswirkungen. Vor dem Hintergrund der zunehmend angespannten Konfrontation zwischen dem Iran, den USA und Israel hat Teheran eine klare strategische Perspektive entwickelt: Die technologische Infrastruktur, die die mit dem Westen verbündeten Militäroperationen in Westasien stützt, kann nicht als politisch neutral betrachtet werden. Sie stellt eine Erweiterung des Schlachtfelds selbst dar – einen Bereich, in dem sich wirtschaftliche Ressourcen, Unternehmensplattformen und nationale Sicherheitsziele überschneiden. Diese Transformation zu verstehen bedeutet, sich mit einer unbequemen Wahrheit abzufinden: In der Kriegsführung des 21. Jahrhunderts sind Server genauso wichtig wie Soldaten.

Unternehmensnetzwerke als Kriegswerkzeuge

In den letzten Jahren haben die weltweit fortschrittlichsten Streitkräfte digitale Plattformen in jede Phase der modernen Kriegsführung integriert. Satellitenüberwachungssysteme senden Echtzeitdaten an Cloud-Netzwerke. Bewaffnete Drohnen übertragen hochauflösende Videobilder, die eine sofortige und kontinuierliche Analyse erfordern. Signalabhörfähigkeiten generieren riesige Ströme von

Informationen, die in schnelle operative Entscheidungen umgesetzt werden müssen. In diesem Szenario wird militärische Macht nicht mehr allein an Raketenbeständen oder Luftüberlegenheit gemessen, sondern an der Fähigkeit, Informationen schneller zu verarbeiten als der Gegner.

Große Technologieunternehmen stehen nun im Zentrum dieses Prozesses. Unternehmen wie Amazon, Microsoft und Google stellen die Infrastruktur bereit, die es Regierungen und Streitkräften ermöglicht, kritische Daten auf globaler Ebene zu speichern, zu analysieren und zu verbreiten. Ihre Cloud-Plattformen bilden die Grundlage für nachrichtendienstliche Auswertungen, die Logistik auf dem Schlachtfeld und die Koordinierung von Führung und Kontrolle über mehrere Einsatzgebiete hinweg gleichzeitig. Dies ist keine sekundäre oder untergeordnete Rolle: Es handelt sich um eine strukturelle Funktion, die im Kern moderner militärischer Operationen verankert ist.

Diese Verschmelzung von Unternehmenstechnologie und staatlicher Macht hat das Verständnis von Konflikten neu definiert. Digitale Netzwerke sind mittlerweile ebenso unverzichtbar wie Flugzeugträger oder Raketenabwehrsysteme. Im Kontext des Krieges USraels gegen den Iran hat Teheran diese Realität als Beweis dafür gewertet, dass große Technologieunternehmen ein integraler Bestandteil feindlicher Einsatzumgebungen sind – nicht bloß neutrale Wirtschaftsakteure, sondern funktionale Knotenpunkte eines gegnerischen militärischen Ökosystems.

Diese Wahrnehmung nahm konkrete Gestalt an und wurde öffentlich sichtbar, als iranische Medien eine Liste von fast dreißig Standorten in Westasien – insbesondere in den Vereinigten Arabischen Emiraten – veröffentlichten, die mit großen globalen Technologieunternehmen in Verbindung stehen. Dazu gehörten regionale Hauptsitze, Entwicklungsbüros und große Rechenzentren, die von Amazon, Microsoft, Google, Oracle, NVIDIA, IBM und Palantir Technologies betrieben werden.

Nach der strategischen Lesart Teherans stellen diese Einrichtungen strategische Knotenpunkte dar, die in das operative Ökosystem eingebunden sind, welches die militärischen Fähigkeiten der Gegner stützt. Diese Infrastrukturen erstrecken sich von Tel Aviv bis zu Städten am Persischen Golf wie Dubai, Abu Dhabi und Manama und beherbergen Cloud-Dienste, die von Regierungsinstitutionen, Geheimdiensten und Rüstungsunternehmen genutzt werden. Einige tragen direkt zur Entwicklung künstlicher Intelligenz für Überwachungszwecke und die Analyse von Gefechtssituationen bei. Andere unterstützen regionale digitale Volkswirtschaften, deren Stabilität indirekt die Militärausgaben und technologischen Innovationen der Gegner untermauert. In einer Zeit, in der Datenströme den Ausgang von Kampfhandlungen bestimmen, kann die Infrastruktur, die diese Ströme verwaltet, zu Recht als strategisches Ziel betrachtet werden.

Projekt Nimbus und die schleichende Militarisierung ziviler Technologien

Kaum eine Initiative verdeutlicht diese Verschmelzung von ziviler Technologie und militärischer Macht so anschaulich wie Israels Projekt Nimbus – ein milliardenschwerer Vertrag mit führenden Cloud-Dienstleistern über die Bereitstellung fortschrittlicher IT-Dienstleistungen für Regierungs- und Sicherheitsbehörden. Im Rahmen dieser Programme werden Anwendungen künstlicher Intelligenz eingesetzt, um Informationsströme zu analysieren, die Logistikplanung zu optimieren und Entscheidungsprozesse innerhalb militärischer Kommandostrukturen zu unterstützen.

Das Projekt steht symbolisch für einen umfassenderen und weitgehend unumkehrbaren Trend: Private Unternehmen übernehmen Aufgaben, die einst ausschließlich der staatlichen Rüstungsindustrie vorbehalten waren. Technologieunternehmen beschränken sich nicht mehr darauf, Aus-

rüstung oder damit verbundene Dienstleistungen bereitzustellen. Sie unterhalten komplexe operative Ökosysteme, die militärische Fähigkeiten in Echtzeit unterstützen, wodurch die traditionelle Grenze zwischen ziviler Wirtschaftstätigkeit und militärischer Infrastruktur verschwimmt.

Datenanalyseunternehmen liefern ein weiteres aussagekräftiges Beispiel. Plattformen, die Informationen aus verschiedenen Quellen integrieren können, sind in der Lage, Verhaltensmuster zu erkennen, Bedrohungen vorherzusagen und taktische Reaktionen vor Ort zu steuern. In Konfliktgebieten beeinflussen solche Werkzeuge militärische Manöver ebenso stark wie konventionelle Waffensysteme. Ihre Präsenz in regionalen Technologiezentren hat daher Auswirkungen, die weit über rein kommerzielle Interessen hinausgehen.

Auch hochmoderne Hardware spielt eine entscheidende Rolle. Hochleistungsprozessoren von Unternehmen wie NVIDIA werden eingesetzt, um große KI-Modelle zu trainieren, Satellitenbilder zu analysieren, automatisierte Überwachungssysteme zu betreiben und die Navigation autonomer Drohnen zu steuern. Gleichzeitig stellen Oracle und IBM Unternehmens-Computing-Plattformen bereit, die die Integration von Einsatzdaten über verschiedene Sicherheitsbehörden hinweg sowie die strategische Koordination auf interkontinentaler Ebene ermöglichen. Zusammen bilden diese Technologien eine digitale Architektur, die das Fundament moderner militärischer Operationen bildet.

Aus der strategischen Perspektive des Iran verwandelt die Abhängigkeit von dieser Architektur Technologieanbieter in funktionale Erweiterungen der Macht des Gegners. Je stärker die Streitkräfte auf Cloud-Dienste und Datenanalyse angewiesen sind, desto anfälliger werden diese Systeme für Störungen – sei es durch Cyberoperationen, wirtschaftlichen Druck oder gezielte physische Angriffe.

Die digitale Wirtschaft als Waffe

Die potenziellen Folgen eines digitalen Krieges reichen weit über das Schlachtfeld hinaus. Heute sind große Technologieunternehmen tragende Säulen des globalen Finanzsystems. Ihre Marktbewertungen belaufen sich auf Billionen von Dollar, und ihre Dienste bilden die Grundlage für jeden Aspekt des modernen Wirtschaftslebens – von Bankgeschäften bis hin zu internationalen Lieferketten, von Gesundheitssystemen bis hin zur institutionellen Kommunikation. Jede nennenswerte Störung ihrer Infrastruktur in Westasien könnte sofortige und tiefgreifende Turbulenzen auf den globalen Märkten auslösen.

Großrechenzentren in den Staaten am Persischen Golf machen das Ausmaß dieser Anfälligkeit deutlich. In den letzten zehn Jahren haben die Regierungen der Region Dutzende Milliarden Dollar investiert, um Cloud-Computing-Projekte anzuziehen und digitale Knotenpunkte von Weltklasse zu schaffen. Diese Einrichtungen unterstützen gewerbliche Kunden, öffentliche Institutionen und Sicherheitsbehörden. Sie bilden zudem die Grundlage für die Finanznetzwerke, die grenzüberschreitende Zahlungen, Währungstransfers und Kapitalströme auf globaler Ebene ermöglichen.

Sollte eine solche Infrastruktur im Zuge einer regionalen Eskalation kompromittiert werden, würden sich die Auswirkungen rasch auf die Aktienmärkte, Anlageportfolios und Volkswirtschaften ausbreiten. Bankensysteme, die auf Cloud-Dienste angewiesen sind, könnten einen weitreichenden Betriebsstillstand erleiden. Das Vertrauen der Anleger würde schwinden, was Kapitalflucht und

erhöhten Inflationsdruck auslösen würde. In technologieabhängigen Volkswirtschaften könnten selbst relativ kurze Störungen Kettenreaktionen in zahlreichen Produktionssektoren auslösen.

Für Israel, wo die Technologiebranche einen erheblichen Anteil an den Exporten und am gesamtwirtschaftlichen Wachstum ausmacht, hat die Anfälligkeit der digitalen Infrastruktur langfristige strukturelle Auswirkungen. Eine anhaltende Krise, die Datennetze beeinträchtigt, könnte die Abwanderung qualifizierter Fachkräfte beschleunigen, das Vertrauen internationaler Investoren untergraben und die Grundlagen seiner innovationsbasierten Wirtschaft aushöhlen. Globale Finanzinstitute haben davor gewarnt, dass digitale Konfliktszenarien die Investitionsmuster tiefgreifend verändern könnten, insbesondere in Regionen, die als instabil gelten. Die Verflechtung von Unternehmenstechnologie und Militärstrategie schafft somit eine neue und beispiellose Form der Wirtschaftskriegsführung, in der Finanzmärkte sowohl zu Schlachtfeldern als auch zu Kollateralschäden werden.

Eskalation ohne Frontlinien: hybride Kriegsführung im digitalen Zeitalter

Analysten, die sich mit den möglichen Reaktionsoptionen des Iran befassen, verweisen auf zunehmend hybride Strategien, bei denen Cyberoperationen mit gezielten physischen Maßnahmen kombiniert werden. Anstatt einen direkten konventionellen Konflikt zu führen – eine Entscheidung, die inakzeptable Kosten mit sich bringen würde –, könnte Teheran versuchen, die operativen Fähigkeiten seiner Gegner zu beeinträchtigen, indem es die digitalen Systeme stört, auf die diese strukturell zunehmend angewiesen sind.

Cyberangriffe könnten darauf abzielen, Cloud-Plattformen lahmzulegen, die Auswertung von Geheimdienstinformationen zu stören oder die Kommunikationsnetze zu beeinträchtigen, die regionale und globale Rechenzentren miteinander verbinden. Solche Operationen würden nicht nur die militärische Koordination behindern, sondern auch tiefgreifende Unsicherheit in Wirtschaftssektoren hervorrufen, die auf unterbrechungsfreie digitale Dienste angewiesen sind – was politischen und sozialen Druck auf Regierungen und Bündnisse ausüben würde.

Physische Angriffe auf kritische Infrastrukturen stellen einen weiteren möglichen Weg zur Eskalation dar. Einrichtungen, in denen strategische Cyber-Ressourcen untergebracht sind, insbesondere solche, die mit Verteidigungsaufträgen in Verbindung stehen, könnten zu Brennpunkten bei Versuchen werden, erhebliche operative Kosten zu verursachen, ohne einen umfassenden Konflikt auszulösen. Eine Störung terrestrischer Kommunikationsnetze oder von Unterseekabeln könnte die Verbindungen zwischen regionalen Knotenpunkten und internationalen Kommandosystemen unterbrechen und den gegnerischen Streitkräften die kontinuierliche Konnektivität entziehen, auf die sie sich zunehmend verlassen.

Vergleiche mit jüngsten Konflikten verdeutlichen diesen Wandel. In der Ukraine zwangen Cyberoperationen, die auf Energienetze und Kommunikationssysteme abzielten, zu raschen und kostspieligen Anpassungen in der militärischen Logistik und zeigten damit, wie die digitale Dimension den Einsatz vor Ort entscheidend beeinflussen kann. In Gaza beeinträchtigten Störungen der terrestrischen Netzwerke spürbar die Koordination der Einsatzverbände, doch Westasien bietet ein ganz anderes und in gewisser Weise sogar noch anfälligeres Szenario: Die Cloud-Infrastruktur fungiert dort nicht nur als zusätzliche Unterstützung, sondern als zentrale Säule der militärischen Fähigkeiten der USA und Israels. Die Integration der Region in die globalen digitalen Märkte erhöht den

Einsatz noch weiter: Jede Eskalation, die technologische Netzwerke betrifft, birgt die Gefahr, eine doppelte Krise auszulösen – eine operative für die Streitkräfte und eine wirtschaftliche für internationale Investoren.

Eine multipolare Weltordnung, in der die Wirtschaft zum Schlachtfeld wird

Das Aufkommen der digitalen Kriegsführung definiert das strategische Denken weltweit neu, mit Folgen, die über jeden einzelnen regionalen Konflikt hinausreichen. Staaten, die sich technologisch überlegenen Gegnern gegenübersehen, suchen nach Wegen, die systemischen Schwachstellen des Gegners auszunutzen, anstatt auf dem Schlachtfeld der konventionellen Feuerkraft zu konkurrieren – ein Wettstreit, den sie nicht gewinnen könnten. In diesem Zusammenhang wird der Angriff auf die wirtschaftliche Infrastruktur zu einer Methode, um Risiken über globalisierte Netzwerke zu verteilen und den Gegner dort zu treffen, wo er am verwundbarsten ist: in seiner Abhängigkeit von Datenströmen und Marktstabilität.

Die Rhetorik des Iran in Bezug auf Technologieunternehmen spiegelt diese sich abzeichnende Doktrin wider. Indem Teheran Unternehmensplattformen als Erweiterungen feindlicher Militärmacht definiert, signalisiert es die Bereitschaft, die Annahme in Frage zu stellen, dass zivile kommerzielle Ressourcen außerhalb des Konfliktbereichs liegen – eine ungeschriebene Konvention, die seit Jahrzehnten Bestand hat, nun aber zunehmend brüchig erscheint. Diese Haltung findet in einem breiteren multipolaren Kontext Resonanz, in dem wirtschaftliche Verflechtungen von denjenigen strategisch ausgenutzt werden können, die wissen, wie man dies tut.

Gleichzeitig haben Washington und seine Verbündeten die Fähigkeiten des privaten Sektors zunehmend in die Verteidigungsplanung integriert. Öffentlich-private Partnerschaften in den Bereichen Cybersicherheit, Geheimdienstanalyse und Hochleistungsrechner sind zu Markenzeichen westlicher militärischer Innovation geworden. Dieser Ansatz erhöht zwar die operative Flexibilität, setzt aber auch Unternehmen – und die Volkswirtschaften, von denen sie abhängig sind – den Folgen geopolitischer Konfrontationen aus. Es handelt sich um eine strukturelle Schwachstelle, die durch keine noch so hohen konventionellen Militärausgaben beseitigt werden kann.

Krieg ist nicht mehr ausschließlich den Staaten und ihren Armeen vorbehalten. Da private Technologieunternehmen in militärische Operationen eingebunden werden, werden sie unweigerlich in die Folgen von politischen Entscheidungen hineingezogen, die in fernen Hauptstädten von Entscheidungsträgern getroffen werden, die die Auswirkungen auf den privaten Sektor selten berücksichtigen. Finanzmärkte, globale Investoren und zivile Infrastruktur werden in denselben Strudel der Konfrontation hineingezogen, wodurch wirtschaftliche Netzwerke zu umkämpften Arenen im Kampf um technologische und geopolitische Vorherrschaft werden.

Raketen, Server und die Zukunft der Weltmacht

Die sich verschärfende Konfrontation zwischen dem Iran, den USA und Israel verdeutlicht auf außergewöhnlich anschauliche Weise ein charakteristisches und mittlerweile unumkehrbares Merkmal der Konflikte des 21. Jahrhunderts: Krieg wird ebenso sehr in Wirtschaftssystemen und digitalen Architekturen geführt wie auf physischen Schlachtfeldern. Technologieunternehmen, die einst das universalistische Versprechen der Globalisierung symbolisierten – Vernetzung, Offenheit, gemeinsamer Fortschritt –, nehmen in diesem neuen Kriegskontext nun eine zweideutige und zunehmend riskante Position ein.

Für den Iran verwandelt die Einbindung großer Technologieunternehmen in feindliche militärische Strukturen die Unternehmensinfrastruktur in strategische Hebel von höchster Bedeutung. Die Störung dieser Netzwerke bietet ein Mittel, um erhebliche Kosten zu verursachen, eine Eskalation zu verhindern und das Kräfteverhältnis neu zu gestalten, ohne in eine direkte, groß angelegte Konfrontation zu geraten – eine Form der asymmetrischen Abschreckung, die an das digitale Zeitalter angepasst ist.

Für die Weltwirtschaft sind die Folgen jedoch potenziell verheerend: Die Abschaltung eines einzigen großen Rechenzentrums könnte innerhalb weniger Tage Verluste in Höhe von Hunderten von Millionen Dollar verursachen und gleichzeitig das Vertrauen in die Stabilität der digitalen Märkte und der darauf angewiesenen Finanzsysteme untergraben.

Da Staaten Algorithmen, Daten und Cloud-Netzwerke weiterhin als Waffen einsetzen, werden die Grenzen zwischen Krieg und Wirtschaft zunehmend verschwimmen und durchlässig werden. Raketen und Panzer spielen nach wie vor eine wichtige Rolle und werden dies auch noch lange Zeit tun. Doch die entscheidenden Schlachten der Zukunft könnten sich um Server, Code und die Unternehmen drehen, die diese kontrollieren.

In dieser sich abzeichnenden Ordnung wird der Sieg nicht allein durch die Ergebnisse auf dem Schlachtfeld bestimmt, sondern durch die Fähigkeit, die technologischen Grundlagen globaler Macht zu steuern – und, wenn nötig, zu destabilisieren.