https://www.geopolitika.ru/en/article/israels-tech-tactics-and-future-total-war

Israels Tech-Taktik und die Zukunft des totalen Krieges

8. Juli 2025 | Alexander Dugin

Seit Beginn des palästinensisch-israelischen Konflikts im Gazastreifen – fast unmittelbar nach dem Angriff der Hamas auf Israel während der Operation „Al-Aqsa-Flut“, der eine Kettenreaktion nachfolgender Ereignisse auslöste – sind wir Zeugen des Einsatzes von Militärtechnologien durch Israel geworden, die zuvor noch nie in Aktion zu sehen waren. Diese Technologien spielten eine entscheidende Rolle bei der Sicherung des israelischen Erfolgs in mehreren militärischen und politischen Operationen.

Sie beinhalteten den Einsatz von Kommunikationsgeräten, Computern, Mobiltelefonen und sogar Pagern, um dem Feind empfindliche, ja kritische Verluste zuzufügen. Diese Taktik war eng mit Raketenangriffen und Kampfdrohnen verwoben. Außerdem ist jetzt klar, dass Israel aktiv die Deepfake-Technologie eingesetzt hat.

Zusammengenommen haben diese Faktoren das Wesen der modernen Kriegsführung grundlegend verändert. Israels Gegner im Nahen Osten waren auf diesen Wandel, der sich als entscheidend für den Verlauf des Konflikts erwies, völlig unvorbereitet. In konventioneller militärischer Hinsicht waren Israel und seine regionalen Gegner in etwa gleich stark – und in der Guerillataktik hatten Gruppen wie die libanesische Hisbollah sogar die Oberhand, wie sich im Libanonkrieg 2006 zeigte. Mit der Einführung dieses neuen technologischen Faktors änderte sich das Kräfteverhältnis jedoch dramatisch.

Um welche neuen Technologien und Methoden handelte es sich dabei? In erster Linie handelte es sich um eine radikal fortschrittliche Überwachungssoftware. Den Israelis gelang es, in praktisch jedem elektronischen Gerät des Gegners ein Ortungsprogramm zu installieren. Bewegungen, Gespräche, Treffen und der Informationsaustausch zwischen Palästinensern, Syrern, Libanesen, Irakern und Iranern – also allen, die für Israel auch nur am Rande von Bedeutung waren – waren für den israelischen Geheimdienst vollständig sichtbar.

In seinem 2019 erschienenen Buch „Das Imperium und die fünf Könige“ beklagte der Globalisierungsforscher Bernard-Henri Lévy den schrittweisen Rückzug des Westens aus dem Nahen Osten (insbesondere aus dem Irak) und stellte fest, dass die einzige Entschädigung für die Aufgabe solcher strategischer Positionen die inzwischen hochentwickelten Überwachungsfähigkeiten des Westens seien, die in der Lage seien, selbst das kleinste Detail in den geräumten Gebieten zu erkennen.

Lévy, ein aggressiver Imperialist, hielt dies für unzureichend – ein Zeichen von Schwäche und Passivität. Er hätte eine direkte physische Kontrolle der islamischen Welt durch den Westen und Israel vorgezogen (daher auch der Titel des Buches, der sich auf den Krieg des alten Israel gegen eine Koalition von fünf kanaanitischen Königen bezieht, die die Israeliten besiegten und unterwarfen). Doch Lévys Hinweis auf die Überwachung war scharfsinnig. Diese wurde ab 2023 zum entscheidenden Faktor.

Kommunikationssysteme und vernetzte Geräte – elektronisch, lokal und anderweitig – wurden in Israels Händen zu tödlichen Waffen, die den Ausgang von Operationen im Gazastreifen, im Libanon, in Syrien und im jüngsten 12-Tage-Krieg mit dem Iran bestimmten. Die Unterstützung durch die USA und andere westliche Staaten war erheblich, aber der entscheidende Vorteil lag in der neuen Strategie. Israel gelang es, die vollständige Kontrolle über die Netzwerke seiner Feinde zu erlangen und Telefone, Pager und verschiedene elektronische Geräte in Waffen zu verwandeln. Einige Pager, die für Hisbollah-Agenten bestimmt waren (die Mobiltelefonen misstrauten), wurden mit Sprengstoff bestückt. Libanesischen Berichten zufolge explodierten nicht nur Pager, sondern auch Mobiltelefone, Elektroroller, Gegensprechanlagen und Aufzugstafeln. Die genaue Beschaffenheit dieser Technologie bleibt unklar, aber wenn sie existiert und Israel sie besitzt, stellt sie ein noch nie dagewesenes Risiko dar.

Eine weitere Komponente waren Drohnen, die auf der Grundlage von durch Überwachung gewonnenen Zieldaten gestartet wurden – oft aus dem gegnerischen Gebiet heraus. Diese Taktik wurde erstmals im Juli 2024 bekannt, als der Hamas-Führer Ismail Haniyeh im Iran ausgeschaltet wurde. Ähnliche Methoden wurden anschließend nicht nur im Gazastreifen, sondern auch in anderen Ländern eingesetzt, um Hamas-Führer zu töten. Dank der elektronischen Überwachung hatten die Israelis ihre Ziele immer im Blick; der Rest war reine Hinrichtung. Die Drohnen konnten von Israel aus oder aus vorbereiteten Verstecken im Ausland gestartet werden.

Es ist sogar möglich, dass die Sabotageaktion, die zum Tod des iranischen Präsidenten Ebrahim Raisi führte, mit einem Pager und Überwachungstechnologie durchgeführt wurde. Raisi war ein konservativer und entschiedener Gegner Israels. Die iranischen Behörden konnten die Ursache des Hubschrauberabsturzes zwar nicht feststellen, doch die Ereignisse des Zwölf-Tage-Krieges könnten den Grund dafür erklären – sie verfügten einfach nicht über die erforderliche Technologie und wussten nicht, wie solche Systeme funktionieren.

Nach der Ausschaltung der Hamas-Führung richtete Israel sein Augenmerk auf die Hisbollah. Durch gezielte Angriffe wurden Scheich Hassan Nasrallah und praktisch die gesamte Führung der Hisbollah, die einst eine ernsthafte Bedrohung für Israel darstellte, getötet. In Kombination mit den explodierenden Pagern und Geräten wurden diese Attentate und sogar Massentötungen von Hisbollah-Mitgliedern außerordentlich effektiv. Es folgten präzise Drohnen- und Raketenangriffe – nicht wahllos, sondern auf der Grundlage von Zielen, die durch elektronische Überwachung ermittelt wurden. Die Israelis planten diese Operationen minutiös und begannen mit der Ausrottung von oben

nach unten: Zuerst wurde die oberste – religiöse und militärisch-politische – Führungsebene eliminiert, dann die zweite und dritte Ebene und so weiter durch die Reihen.

In Syrien war es der Mossad, der die ISIS-nahe al-Sharaa an die Macht brachte, einen Regimewechsel herbeiführte und Präsident Bashar al-Assad mit denselben Techniken stürzte. Israel erlangte die volle Kontrolle über die syrische Militärkommunikation. Deepfakes wurden in großem Umfang eingesetzt. Befehle und Anweisungen – manchmal widersprüchlich – wurden an rangniedrigere Befehlshaber geschickt, angeblich von der syrischen Führungsspitze, wobei sogar die Stimme von Assad selbst imitiert wurde. Dazu gehörten Befehle zum Rückzug, zur Verlegung in sinnlose Stellungen oder zum Beschuss falscher Ziele.

Der Regimewechsel wurde weniger durch konventionelle militärische Gewalt als durch vernetzte Technologien erreicht. Israel festigte außerdem seine Stellung auf den Golanhöhen, dehnte seine Kontrollzone auf die näher an Damaskus gelegenen drusischen Gebiete aus und zerstörte – mit Hilfe von Drohnen und Raketen – jede syrische Militäreinrichtung, die auch nur im Entferntesten eine Gefahr darstellte. Zuvor waren die Hisbollah und die iranischen Streitkräfte (insbesondere die IRGC-Einheiten) in Syrien bereits genau ins Visier genommen und nach Beginn des Al-Sharaa-Aufstands zum Rückzug gezwungen worden.

Als nächstes kam der Iran. Auch hier wurde die gleiche Strategie angewandt. In den ersten Stunden des 12-tägigen Krieges eliminierte Israel fast die gesamte oberste iranische Militärführung – den Generalstabschef, den IRGC-Kommandeur und führende Atomwissenschaftler – sowie deren Familien, **einschließlich kleiner Kinder**. Dies geschah zum Teil durch Präzisionsraketenangriffe, zum Teil durch Drohnen, die aus dem Inneren des Irans mit Hilfe von zuvor deponierten Verstecken gestartet wurden. Die Drohnen wurden von afghanischen Migranten gestartet, die israelische Anweisungen befolgten, bescheidene Summen erhielten und von den israelischen Planern als entbehrlich angesehen wurden.

Die anschließenden Raketenangriffe richteten sich gegen die nukleare Infrastruktur des Irans und führten zu einem Regimewechsel. Damit dies alles gelingen konnte, brauchte Israel die vollständige Kontrolle über jede einzelne iranische Person, die als potenzielle Bedrohung oder Interesse angesehen wurde – und auch dies geschah durch elektronische Geräte. Gegen die jemenitischen Houthis war diese Strategie weniger effektiv, aber auch sie wurden gelegentlich mit Präzisionsangriffen getroffen, die schweren Schaden anrichteten.

Auf diese Weise haben sich völlig neue Formen der tödlichen Kriegsführung herausgebildet. Israel verfügt über Technologien, die es ihm ermöglichen, seinen Feinden bisher unvorstellbare Schäden zuzufügen. Wir sind in eine völlig neue Ära des Krieges eingetreten.

In der Anfangsphase der militärischen Sonderoperation (SMO) stießen wir unerwartet auf das Problem der Drohnen und der Kommunikation. Doch was wir jetzt in Israel sehen, stellt eine weitaus fortgeschrittenere Stufe dar. Wenn Sie oder Ihre Familienmitglieder ein elektronisches Gerät besitzen und mit den Interessen Israels in Konflikt geraten, können Sie chirurgisch, effizient und in jedem Moment eliminiert werden. Dies ist die erschreckende Schlussfolgerung aus dem, was wir gerade im Nahen Osten erlebt haben.

Ein weiteres Problem ist die Ausschaltung von feindlichen Flotten und Seehäfen. Auch hier stellen Wasserdrohnentechnologien – die noch nicht vollständig eingesetzt werden – eine kolossale Gefahr dar, insbesondere in Verbindung mit fortschrittlichen Überwachungssystemen.

Wir haben es also mit einem ganzen Block von neuen Bedrohungen zu tun. Der nächste Punkt: Israel ist der engste Verbündete der USA und des gesamten Westens. Einige sehen Israel als geopolitischen Stellvertreter der USA, während andere – insbesondere Israelis – die USA als unterwürfigen Golem unter israelischem Kommando sehen. Wie auch immer, das Wesentliche ist dasselbe: Die Technologien, die Israel in der Kriegsführung gegen seine regionalen Gegner so effektiv eingesetzt hat, sind den USA und dem Westen zweifellos bekannt und zugänglich. Es ist in der Tat unklar, ob es sich dabei um rein israelische Erfindungen handelt. Vielleicht stammen sie von der CIA, dem Pentagon, Palantir oder dem MI6 – oder sie wurden gemeinsam entwickelt. Das spielt kaum eine Rolle. Der Punkt ist: Der Westen verfügt über diese Waffen und beherrscht diese Strategien und Technologien.

Russland befindet sich nicht im Krieg mit Israel (obwohl wir nicht vergessen sollten, dass der Iran unser Verbündeter ist), so dass man meinen könnte, wir seien vor solchen Taktiken sicher. Vielleicht. Allerdings befinden wir uns in der Ukraine unbestreitbar im Krieg mit dem kollektiven Westen – und die Ukraine ist eindeutig ein Stellvertreter, ein Werkzeug des kollektiven Westens. Daraus ergibt sich die einfache und erschreckende Schlussfolgerung: Diese tödliche Technologie kann jederzeit gegen Russland eingesetzt werden.

Wenn wir uns die von ukrainischen Saboteuren in Russland verübten Terroranschläge ansehen – gegen Daria Dugina (und mich), gegen Wladlen Tatarski und Sachar Prilepin, gegen russische Generäle wie Moskalyok und Kirillow und auch den Anschlag auf das Krokus-Rathaus, an dem von Kiew angeworbene Migranten beteiligt waren –, dann muss der jüngste Drohnenangriff auf Russlands nukleare Triade von russischem Territorium aus in diesem Kontext gesehen werden. In einer kritischen Situation könnte eine solche Strategie in vollem Umfang zum Einsatz kommen – oder wurde möglicherweise bereits eingesetzt, wenn auch in begrenzter Form.

Es stellen sich logische Fragen: Verfügen wir über ähnliche Waffensysteme? Sind wir in feindliche Geräte und Vorrichtungen eingedrungen – nicht nur in die der Ukraine, sondern auch in die der USA und der NATO? Verfügen wir andererseits über angemessene Verteidigungsmaßnahmen gegen solche Angriffe und Strategien?

Natürlich arbeiten unsere Top-Spezialisten eifrig daran, die Sicherheit des Präsidenten – unserer wichtigsten Ressource im Krieg gegen den Westen – zu gewährleisten. Deshalb besitzt er auch keine elektronischen Geräte – und das ist auch gut so. Dennoch digitalisieren und elektrifizieren wir weiterhin alles und verlassen uns dabei auf künstliche Intelligenz, die, wie andere vernetzte Technologien auch, bereits als Waffe eingesetzt werden kann – oder leicht dazu werden könnte. Kann KI tödlich sein? Die Antwort liegt nach den Erfahrungen der Libanesen und Iraner auf der Hand: Wenn Telefone und Pager tödlich sein können, dann kann KI unter bestimmten Bedingungen durchaus als Waffe eingesetzt werden. Durch KI erzeugte Deepfakes sind bereits zu Waffen geworden.

Sind wir uns darüber hinaus bewusst, dass Netzwerkstrukturen leicht in Einwanderergemeinschaften eingebettet werden können, insbesondere bei illegalen Einwanderern? Sie sind fertige

technische Agenten. Israel hätte ohne ein elitenbasiertes Agentennetz vor Ort niemals so tiefgreifende Sabotagenetzwerke in Gesellschaften einrichten können.

Und schließlich: Verfügt China über solche Technologien für militärische Netzwerke? Im Moment steht China vor einer kritischen Entscheidung – ob es sich auf eine offene Konfrontation mit dem Westen im Iran und im Nahen Osten einlassen soll, wo der Westen gezielte Angriffe auf chinesische Energie- und Verkehrsknotenpunkte durchführt. Wir werden es wahrscheinlich bald herausfinden.

Unabhängig davon ist dies heute die größte Bedrohung für das heutige Russland. Alles andere können wir bewältigen. Doch hier stehen wir vor etwas völlig Neuem – und wenn wir in einem kritischen Moment unvorbereitet sind, könnten die Folgen wirklich fatal sein.